SNI

Standar Nasional Indonesia

SNI 7512:2008

Teknologi informasi – Teknik keamanan – Pengelolaan insiden keamanan Informasi

"Information technology – Security techniques – Information security incident management **(ISO/IEC TR 18044:2004, MOD)"**

ICS 35.040

Badan Standardisasi Nasional

BSN
Gd. Manggala Wanabakti
Blok IV, Lt. 3,4,7,10.
Telp. +6221-5747043
Fax. +6221-5747045
Email: dokinfo@bsn.go.id
www.bsn.go.id

Diterbitkan di Jakarta

Daftar isi

Prakata

Standar Nasional Indonesia *Teknologi informasi – Teknik keamanan – Pengelolaan insiden keamanan informasi* diadopsi secara modifikasi dari ISO/IEC TR 18044:2004, *Information technology – Security techniques – Information security incident management*, yang disesuaikan dengan keadaan di Indonesia yang berbeda ketersediaan perangkat hukumnya dengan negara luar. Modifikasi dilakukan terhadap beberapa perbedaan teknis. Pemberian tanda garis vertikal tunggal di samping teks, menunjukkan perbedaan teknis yang terdapat pada SNI. Modifikasi pada butir 5.2.3, perbedaan teknis dijelaskan dalam Lampiran C.

Standar ini disusun oleh Panitia Teknis 35-02, *Komunikasi Digital* dan telah dibahas dalam rapat konsensus di Jakarta pada tanggal 8 Desember 2006, yang dihadiri oleh pihak terkait yaitu produsen, konsumen, pakar di bidangnya dan pemerintah. SNI ini juga telah melalui konsensus nasional yaitu jajak pendapat pada tanggal 27 Agustus – 27 Oktober 2007.

Apabila ada keraguan dalam terjemahan kalimat atau istilah di standar ini, dapat melihat standar aslinya ISO/IEC TR 18044:2004, *Information technology – Security techniques – Information security incident management*.

Teknologi informasi – Teknik keamanan – Pengelolaan insiden keamanan informasi

1 Ruang lingkup

Laporan Teknis (LT) Tipe 3 ini memberikan arahan dan pedoman tentang pengelolaan insiden keamanan informasi untuk pengelola keamanan informasi, dan pengelola sistem, layanan dan jaringan informasi.

LT ini berisi 11 klausul dan diatur dengan cara berikut. Klausul 1 menguraikan ruang lingkup dan diikuti oleh daftar acuan dalam klausul 2 dan istilah dan definisi dalam klausul 3. klausul 4 memberikan beberapa latar belakang mengenai pengelolaan insiden keamanan informasi, diikuti oleh ringkasan manfaat dan hal-hal penting dalam klausul 5. Contoh dari insiden keamanan informasi dan penyebabnya kemudian diberikan dalam klausul 6. Perencanaan dan persiapan pengelolaan insiden keamanan informasi, termasuk produksi dokumen, diuraikan dalam klausul 7. Penggunaan operasional rencana pengelolaan insiden keamanan informasi diuraikan dalam klausul 8. Tahap tinjauan pengelolaan keamanan informasi, termasuk identifikasi pengalaman (pelajaran yang dipelajari) dan peningkatan keamanan dan rencana pengelolaan insiden keamanan informasi, diuraikan dalam klausul 9. Tahap perbaikan, yaitu. pembuatan perbaikan teridentifikasi keamanan dan rencana pengelolaan insiden keamanan informasi, diuraikan dalam klausul 10. Akhirnya, LT menyimpulkan dengan suatu ringkasan yang pendek dalam klausul 11. Lampiran A berisi contoh laporan kejadian dan insiden keamanan informasi, sedangkan Lampiran B berisi beberapa contoh pedoman umum untuk menilai dampak dari insiden keamanan informasi, untuk dimasukkan dalam formulir pelaporan.

2 Acuan normatif

Dokumen yang diacu berikut ini sangat dibutuhkan untuk penerapan dari dokumen ini. Untuk acuan bertanggal, hanya edisi yang dikutip yang berlaku. Untuk acuan yang tak bertanggal, berlaku edisi terakhir dokumen yang dijadikan acuan (termasuk amandemennya).

ISO/IEC 13335-1:2004, *IT security techniques - Management of information and communications technology security - Part 1: Concepts and modelsfor information and communications technology security management.*

ISO/IEC 17799:2000, *Information technology - Code of practice for information security management.*

3 Istilah dan definisi

Untuk keperluan dokumen ini berlaku istilah dan definisi yang diberikan dalam ISO/IEC 13335-1, ISO/IEC 17799 dan istilah dan definisi seperti di bawah ini:

3.1
perencanaan bisnis berkesinambungan
perencanaan bisnis berkesinambungan adalah proses untuk menjamin bahwa operasi pemulihan akan dilakukan jika terjadi insiden yang tidak dikehendaki atau tidak diduga, yang mampu menimbulkan dampak negatif terhadap kesinambungan fungsi bisnis yang penting dan unsur-unsur pendukungnya. Proses ini harus juga menjamin bahwa pemulihan dapat dicapai sesuai dengan prioritas kebutuhan dan jangka waktu yang diminta, dan sesudah itu semua fungsi bisnis dan unsur-unsur pendukung akan kembali normal.

Unsur-unsur kunci dari proses harus dapat menjamin bahwa rencana dan fasilitas telah tersedia, dan teruji. Unsur-unsur kunci tersebut terdiri dari : informasi, proses bisnis, sistem dan layanan informasi, komunikasi suara dan data, SDM dan fasilitas fisik.

3.2
kejadian keamanan informasi
kejadian keamanan informasi adalah teridentifikasikannya keadaan suatu sistem, layanan atau jaringan yang menunjukkan adanya kemungkinan pelanggaran terhadap kebijakan keamanan informasi atau kegagalan perlindungan, atau situasi yang tak dikenal sebelumnya yang mungkin berhubungan dengan keamanan.

3.3
insiden keamanan informasi
insiden keamanan informasi adalah suatu kejadian tunggal atau serangkaian kejadian keamanan informasi yang tidak diduga atau tidak dikehendaki yang mempunyai kemungkinan besar mengganggu operasi bisnis dan mengancam keamanan informasi. (Contoh insiden keamanan informasi ditunjukkan dalam Klausul 6).

3.4
ISIRT (*Information Security Incident Response Team-Unit Tanggap Insiden Keamanan Informasi*)
ISIRT adalah suatu tim yang terampil,ahli dan dipercaya dari organisasi, yang akan menangani insiden keamanan informasi selama masa tugas mereka. Pada waktu tertentu tim ini bisa ditambah dengan tenaga ahli eksternal, misalnya dari *Computer Emergency Response Team-Unit Tanggap Darurat* (CERT).

3.5
lain-lain
lihat juga definisi dalam ISO/IEC JTC1 SC27 SD6, *Glossary* (Daftar kata).

4 Latar belakang

4.1 Tujuan

Pendekatan yang terencana baik dan terstruktur terhadap pengelolaan insiden keamanan informasi merupakan hal yang sangat penting sebagai bagian utama dari strategi keamanan informasi yang menyeluruh dari suatu organisasi.

Tujuan dari pendekatan ini adalah untuk memastikan bahwa:
- kejadian keamanan informasi dapat dideteksi dan ditangani secara efisien, khususnya dalam pengidentifikasian apakah insiden tersebut perlu dikategorikan sebagai insiden keamanan informasi atau bukan, [1]
- insiden keamanan informasi yang telah teridentifikasi dapat dinilai dan ditanggapi dengan cara yang paling tepat dan efisien,
- dampak yang kurang baik dari insiden keamanan informasi pada organisasi dan operasi bisnisnya dapat diperkecil dengan perlindungan yang sesuai, sebagai bagian dari tanggapan insiden keamanan informasi, mungkin bersamaan dengan unsur-unsur yang relevan dari sebuah rencana kesinambungan bisnis
- pelajaran dapat dengan cepat dipelajari dari insiden keamanan informasi dan cara pengelolaannya. Hal ini untuk meningkatkan kesempatan pencegahan terjadinya insiden

[1] Harus dicatat bahwa sebuah kejadian keamanan informasi mungkin adalah hasil usaha disengaja atau kebetulan untuk melanggar perlindungan keamanan informasi, tetapi dalam banyak kasus kejadian keamanan informasi saja tidak menyiratkan bahwa suatu usaha telah benar-benar berhasil dan oleh karena itu tidak harus berimplikasi pada kerahasiaan, integritas dan/atau ketersediaan, yaitu. tidak semua kejadian keamanan informasi dikategorikan sebagai insiden keamanan informasi.

keamanan informasi di masa depan, meningkatkan implementasi dan penggunaan perlindungan keamanan informasi, serta meningkatkan skema pengelolaan insiden keamanan informasi secara menyeluruh..

4.2 Proses

Untuk mencapai tujuan yang digambarkan dalam butir 4.1. pengelolaan insiden keamanan informasi terdiri dari empat proses yang berbeda:

- Perencanaan dan Persiapan,
- Penggunaan,
- Peninjauan ulang,
- Perbaikan.

(Harus dicatat bahwa proses ini serupa dengan yang dicerminkan dalam model "Perencanaan, Pelaksanaan, Pemeriksaan dan Tindakan" dalam ISO 9000 dan ISO 14000.) Gambaran umum dari proses-proses tersebut ditunjukkan dalam Gambar 1 di bawah.

Gambar 1 – Proses pengelolaan insiden keamanan informasi

4.2.1.1 Perencanaan dan Persiapan

Pengelolaan insiden keamanan informasi yang efektif memerlukan persiapan dan perencanaan yang tepat. Agar tanggapan atas insiden keamanan informasi bisa efektif, perlu tindakan-tindakan sebagai berikut:

- Membuat dan mendokumentasikan kebijakan pengelolaan insiden keamanan informasi dan dapatkan komitmen nyata untuk kebijakan itu dari semua pemangku amanah kunci, terutama sekali pengelola senior,
- Membuat dan mendokumentasikan secara komprehensif skema pengelolaan insiden keamanan informasi untuk mendukung kebijakan pengelolaan insiden keamanan informasi tersebut. Formulir, prosedur dan alat pendukung, untuk pendeteksian, pelaporan, penilaian dan tanggapan atas insiden keamanan informasi, dan rincian skala kerusakan (severity) insiden[2], harus dimasukkan dalam dokumentasi. (Harus dicatat bahwa dalam beberapa organisasi, skema tersebut bisa dianggap sebagai rencana tanggapan terhadap insiden keamanan informasi.),

[2] Skala kesulitan insiden yang digunakan untuk “pentahapan” insiden harus dibentuk. Skala ini bisa, misalnya, “besar” dan “kecil', dengan, biar bagaimanapun juga, keputusan yang didasarkan pada dampak yang kurang baik aktual atau yang diproyeksikan atas operasi bisnis organisasi.

- memutakhirkan keamanan informasi dan kebijakan pengelolaan resiko pada semua tingkat, yaitu, menurut korporat dan untuk masing-masing sistem, layanan dan jaringan, dengan mengacu kepada skema pengelolaan insiden keamanan informasi,
- membentuk suatu struktur organisasi pengelola insiden keamanan informasi yang sesuai, yaitu, ISIRT, dengan peran dan tanggung-jawab yang jelas, yang diberikan kepada personil yang tersedia agar dapat menanggapi semua jenis insiden keamanan informasi yang diketahui secara memadai. Dalam kebanyakan organisasi, ISIRT merupakan suatu tim bayangan (virtual), yang dipimpin oleh seorang manajer senior dan didukung oleh kelompok individu yang mengkhususkan diri pada keahlian tertentu, misalnya dalam penanganan serangan kode yang merusak (*malicious code*), yang akan dipanggil tergantung pada jenis insiden terkait,
- membuat semua personil organisasi menyadari, melalui pengarahan singkat dan/atau mekanisme lainnya, tentang keberadaan skema pengelolaan insiden keamanan informasi, manfaatnya dan bagaimana cara melaporkan suatu insiden keamanan informasi. Pelatihan yang sesuai harus diberikan kepada personil yang bertanggung jawab untuk mengelola skema pengelolaan insiden keamanan informasi, pembuat keputusan yang dilibatkan dalam penentuan apakah kejadian keamanan informasi adalah insiden, dan individu yang dilibatkan dalam penyelidikan insiden tersebut,
- menguji secara menyeluruh skema pengelolaan insiden keamanan informasi tersebut.

Tahap Perencanaan dan Persiapan diuraikan lebih lanjut dalam butir 7.

4.2.2 Penggunaan

Proses-proses berikut ini diperlukan untuk menggunakan skema pengelolaan insiden keamanan informasi:

- pendeteksian dan pelaporan kejadian keamanan informasi (oleh manusia atau sarana otomatis),
- pengumpulan informasi yang berhubungan dengan kejadian keamanan informasi, dan melakukan penilaian informasi tersebut untuk menentukan kejadian apa yang dapat digolongkan sebagai insiden keamanan informasi,
- pembuatan tanggapan atas insiden keamanan informasi:
  - segera, dalam waktu-nyata(real time) atau mendekati waktu-nyata(near real time),
  - jika insiden keamanan informasi berada di bawah kendali, lakukan kegiatan-kegiatan yang mungkin diperlukan dalam waktu yang lebih lambat (sebagai contoh, memudahkan pemulihan sepenuhnya dari suatu kerusakan (disaster)),
  - jika insiden keamanan informasi tidak dapat dikendalikan, perlu mendorong kegiatan penanggulangan 'krisis' (sebagai contoh, memanggil pemadam kebakaran atau mengaktifkan rencana kesinambungan bisnis),
  - mengkomunikasikan adanya insiden keamanan informasi dan rinciannya yang relevan kepada orang-orang dan/atau organisasi internal dan eksternal. (Ini bisa meliputi eskalasi penilaian dan/atau keputusan lebih lanjut, bila diperlukan.),
  - analisis forensik,
  - pencatatanging dengan benar semua kegiatan dan keputusan untuk analisis lebih lanjut,
  - penutupan insiden melalui sebuah resolusi.

Tahap Penggunaan lebih lanjut diuraikan dalam butir 8.

4.2.3 Peninjauan

Setelah insiden keamanan informasi telah diselesaikan/ditutup, perlu dilakukan kegiatan peninjauan yang berikut:

- melaksanakan analisis forensik lebih lanjut, bila diperlukan,

- mengidentifikasikan pelajaran yang diperoleh (pengalaman) dari insiden keamanan informasi,
- mengidentifikasikan perbaikan terhadap pelaksanaan perlindungan keamanan informasi, sebagai hasil dari pelajaran yang diperoleh, baik dari satu atau lebih insiden keamanan informasi,
- mengidentifikasikan perbaikan terhadap skema pengelolaan insiden keamanan informasi secara keseluruhan, sebagai hasil pelajaran yang diperoleh dari peninjauan jaminan mutu terhadap sebuah pendekatan (sebagai contoh, dari tinjauan atas keefektifan proses, prosedur, formulir pelaporan dan/atau struktur organisasi).

Tahap Tinjauan diuraikan lebih jauh dalam butir 9.

4.2.4 Perbaikan

Perlu ditekankan bahwa proses pengelolaan insiden keamanan informasi adalah berulang, dengan perbaikan secara reguler dibuat untuk sejumlah unsur-unsur keamanan informasi dari waktu ke waktu. Perbaikan ini diusulkan atas dasar tinjauan data atas insiden keamanan informasi dan tanggapannya, serta kecenderungan dari waktu ke waktu. Perbaikan ini meliputi:

- perbaikan analisis resiko keamanan informasi organisasi yang ada dan hasil tinjauan pengelola,
- peningkatan skema dari pengelolaan insiden keamanan informasi dan dokumentasinya,
- memulai perbaikan keamanan, yang meliputi implementasi dari perlindungan keamanan. Informasi baru dan/atau yang dimutakhirkan

Tahap Perbaikan diuraikan lebih lanjut dalam butir 10.

5 Manfaat dan isu penting

Klausul ini memberikan informasi tentang:

- manfaat yang akan diperoleh dari skema pengelolaan insiden keamanan informasi yang baik,
- isu penting yang perlu ditangani untuk meyakinkan pengelola senior perusahaan dan personil yang akan melaporkan dan menerima umpan balik dari skema tersebut.

5.1 Manfaat

Organisasi yang menggunakan pendekatan terstruktur terhadap pengelolaan insiden keamanan informasi bisa mendapatkan manfaat yang penting, yang dapat dikelompokkan di bawah ini:

- perbaikan keamanan informasi,
- pengurangan dampak bisnis yang kurang baik, sebagai contoh adalah gangguan dan kerugian keuangan, yang disebabkan sebagai konsekuensi dari insiden keamanan informasi,
- penguatan fokus dari pencegahan insiden keamanan informasi,
- penguatan prioritas dan bukti,
- memberikan kontribusi terhadap justifikasi anggaran dan sumber daya,
- perbaikan pemutakhiran analisis risiko dan hasil manajemen,
- perbaikan terhadap kesadaran keamanan informasi dan materi dari program pelatihan,
- penyediaan masukan untuk kebijakan keamanan informasi dan tinjauan terhadap dokumentasi yang terkait.

Penjelasan untuk setiap topik di atas disampaikan berikut ini.

5.1.1 Perbaikan keamanan

Proses yang terstruktur untuk pendeteksian, pelaporan, penilaian dan pengelolaan insiden keamanan informasi dan insiden yang memungkinkan identifikasi dan tanggapan cepat atas insiden atau kejadian keamanan informasi, dengan begitu meningkatkan keamanan secara keseluruhan melalui identifikasi dan pelaksanakan solusi yang konsisten secara cepat, sehingga dapat disediakannya sarana untuk pencegahan insiden keamanan informasi yang serupa dimasa depan.

5.1.2 Pengurangan dampak bisnis yang kurang baik

Pendekatan yang terstruktur terhadap pengelolaan insiden keamanan informasi dapat membantu mengurangi dampak bisnis potensial yang kurang baik, yang berhubungan dengan insiden keamanan informasi. Dampak ini dapat meliputi kerugian keuangan secara langsung, dan kerugian dalam jangka yang lebih panjang, yang timbul dari rusaknya kredibilitas dan reputasi.

5.1.3 Penguatan fokus pencegahan dari insiden

Penggunaan pendekatan terstruktur terhadap pengelolaan insiden keamanan informasi dapat membantu menciptakan fokus yang lebih baik bagi pencegahan insiden dalam suatu organisasi. Analisis terhadap data insiden terkait memungkinkan identifikasi pola dan kecenderungan, sehingga dapat menfasilitasi fokus yang lebih akurat terhadap pencegahan insiden dan oleh karena itu identifikasi tindakan yang sesuai untuk mencegah terjadinya insiden.

5.1.4 Penguatan prioritas dan bukti

Pendekatan terstruktur kepada pengelolaan insiden keamanan informasi akan menyediakan dasar yang kokoh untuk pemberian prioritas ketika melakukan penyelidikan insiden keamanan informasi.

Jika tidak ada prosedur yang jelas, ada resiko kegiatan penyelidikan bisa dilakukan dengan cara reaktif, menanggapi insiden saat terjadi dan menanggapi "suara paling nyaring" dari manajemen yang terkait. Ini bisa mencegah kegiatan penyelidikan yang diarahkan, dimana mereka sungguh diperlukan dan sesuai dengan prioritas yang ideal.

Prosedur penyelidikan insiden yang jelas dapat membantu memastikan bahwa pengumpulan data dan penanganan data dilakukan secara baik dan secara hukum dapat diterima. Hal Ini merupakan pertimbangan yang penting jika terjadi tuntutan hukum dan tindakan penertiban selanjutnya. Meskipun demikian, harus dimengerti bahwa ada tindakan pemulihan dari suatu insiden keamanan informasi yang mungkin dapat membahayakan integritas bukti yang dikumpulkan.

5.1.5 Anggaran dan sumber daya

Pendekatan yang terstruktur dan terdefinisikan dengan baik dalam pengelolaan insiden keamanan informasi akan membantu membenarkan dan menyederhanakan alokasi anggaran dan sumber daya dalam unit organisasi yang dilibatkan. Lebih lanjut, manfaat akan bertambah untuk skema pengelolaan insiden keamanan informasi itu sendiri, dengan:

- memakai staff yang kurang trampil untuk mengidentifikasi dan menyaring alarm palsu,
- ketentuan arah yang lebih baik untuk kegiatan personil yang trampil,

- penugasan personil trampil hanya untuk proses yang membutuhkan ketrampilan mereka dan hanya pada tahap proses yang memerlukan kontribusi mereka.

Sebagai tambahan, pendekatan terstruktur dalam pengelolaan insiden keamanan informasi dapat meliputi 'time stamping" sehingga dimungkinkan untuk membuat penilaian 'kuantitatif' dari penanganan organisasi terhadap insiden keamanan. Sebagai contoh, adalah mungkin untuk memberikan informasi tentang berapa lama diperlukan untuk menyelesaikan insiden dengan prioritas yang berbeda dan pada platform yang berbeda. Jika ada *bottlenecks* pada proses pengelolaan insiden keamanan informasi, ini juga harus bisa diidentifikasikan.

5.1.6 Analisis dan pengelolaan resiko keamanan informasi

Penggunaan pendekatan terstruktur kepada pengelolaan insiden keamanan informasi akan memudahkan:

- pengumpulan data yang lebih baik untuk membantu pengidentifikasian dan penentuan karakteristik dari berbagai jenis ancaman dan kerentanan yang terkait,
- penyediaan data tentang frekuensi terjadinya berbagai jenis ancaman yang dapat diidentifikasikan.

Data yang diperoleh dari dampak yang kurang baik atas operasi bisnis dari suatu insiden keamanan informasi akan bermanfaat dalam analisis dampak bisnis. Data yang diperoleh dari identifikasi frekuensi timbulnya berbagai jenis ancaman akan sangat membantu mutu penilaian ancaman. Dengan cara yang sama, data yang diperoleh atas kerentanan akan sangat membantu mutu penilaian kerentanan di masa depan.

Data ini akan sangat meningkatkan hasil analisis resiko keamanan informasi dan hasil tinjauan manajemen.

5.1.7 Kesadaran keamanan informasi

Pendekatan terstruktur dalam pengelolaan insiden keamanan informasi akan memberikan informasi yang terfokus untuk program kesadaran keamanan informasi. Informasi yang terfokus akan menyediakan suatu contoh nyata dari informasi yang mampu mempertunjukkan bahwa insiden keamanan informasi benar-benar terjadi pada organisasi, dan tidak selalu "bagi orang lain". Juga dimungkinkan untuk mempertunjukkan manfaat yang berhubungan dengan ketersediaan solusi secara cepat. Lebih jauh lagi, kesadaran seperti itu membantu mengurangi kekeliruan atau kepanikan perorangan jika terjadi insiden keamanan informasi.

5.1.8 Masukan untuk tinjauan kebijakan keamanaan informasi

Data yang diberikan oleh skema pengelolaan insiden keamanan informasi bisa menyediakan masukan yang berharga untuk peninjauan ulang terhadap efektivitas dan perbaikan selanjutnya, dari suatu kebijakan keamanan informasi (dan dokumen keamanan informasi terkait lainnya). Hal ini berlaku juga untuk kebijakan dan dokumen lain yang berlaku baik untuk organisasi maupun untuk sistem, layanan dan jaringan yang berdiri sendiri.

5.2 Isu kunci

Umpan balik atas insiden keamanan informasi yang telah dikelola akan membantu personil untuk memastikan bahwa pekerjaan mereka tetap terfokus pada resiko yang sebenarnya terhadap sistem organisasi, layanan dan jaringan. Umpan balik yang penting tidak bisa seefektif yang disajikan melalui penanganan insiden keamanan informasi jika terjadi atas dasar yang bersifat sementara. Ia dapat disajikan dengan lebih efektif melalui penggunaan skema pengelolaan insiden keamanan informasi terencana dengan baik yang terstruktur

yang menggunakan kerangka umum untuk semua bagian organisasi. Kerangka ini memungkinkan secara berkesinambungan memberikan hasil lebih menyeluruh skema tersebut, dan membuat suatu dasar yang kokoh untuk identifikasi cepat kondisi-kondisi insiden keamanan informasi untuk diwakili sebelum suatu insiden keamanan informasi terjadi, kadang-kadang disebut "siaga".

Pengelolaan dan audit skema pengelolaan keamanan informasi harus memberikan basis untuk kepercayaan yang diperlukan untuk memudahkan keikutsertaan yang lebih luas, dan untuk menghilangkan kekhawatiran perhatian tentang pelestarian keadaan tanpa nama, keamanan dan ketersediaan hasil yang bermanfaat. Sebagai contoh, personil pengelolaan dan operasi perlu yakin bahwa "siaga" akan memberikan informasi yang tepat waktu, relevan, akurat, ringkas dan lengkap.

Organisasi perlu menghindari permasalahan potensial dalam menerapkan skema pengelolaan insiden keamanan informasi, seperti kurangnya hasil yang bermanfaat dan kekhawatiran tentang isu yang terkait dengan provasi. Adalah perlu untuk meyakinkan pemangku amanah bahwa telah diambil langkah-langkah untuk mencegah terjadinya permasalahan seperti itu.

Jadi, sejumlah isu penting harus ditangani untuk mendapatkan skema rencana pengelolaan insiden keamanan informasi yang baik, termasuk:

- komitmen pengelolaan,
- kesadaran,
- aspek hukum dan regulasi,
- efisiensi dan mutu operasional,
- keadaan tanpa nama,
- kerahasiaan,
- operasi yang terpercaya,
- tipologi

Masing-masing isu dibahas di bawah ini.

5.2.1 Komitmen pengelolaan

Memastikan komitmen pengelolaan berlanjut adalah hal penting untuk penerimaan pendekatan terstruktur pengelolaan insiden keamanan informasi. Personil harus mengenali suatu insiden dan mengetahui apa yang harus dikerjakan, dan bahkan memahami manfaat yang luas pendekatan kepada organisasi. Meskipun demikian, kecuali jika pengelola mendukung, sedikit yang akan terjadi. Gagasan tersebut perlu dijual kepada pengelola sehingga organisasi mengikat kepada pengadaan dan pemeliharaankemampuan menanggapi insiden.

5.2.2 Kesadaran

Isu penting lainnya untuk penerimaan pendekatan terstruktur terhadap informasi pengelolaan insiden keamanan adalah kesadaran. Selagi para pemakai harus diminta untuk ambil bagian, jika mereka tidak menyadari tentang bagaimana mereka dan bagian dari organisasi mereka memperoleh manfaat dari keikutsertaan dalam pendekatan terstruktur terhadap pengelolaan insiden keamanan informasi, mereka kemungkinan kecil ambil bagian secara efektif dalam operasinya.

Setiap skema pengelolaan insiden keamanan in harus didampingi oleh dokumen definisi program kesadaran yang meliputi rincian:

- bermanfaat yang diperoleh dari pendekatan terstruktur atas pengelolaan insiden keamanan informasi, atas organisasi dan personilnya,
- informasi insiden yang disimpan dalam, dan keluaran dari, basis data insiden keamanan informasi,
- strategi dan mekanisme untuk program kesadaran, yang tergantung pada organisasi, bisa berdiri sendiri atau bagian dari program kesadaran keamanan informasi yang lebih luas.

5.2.3 Aspek hukum dan regulasi

Aspek hukum dan regulasi tentang pengelolaan insiden keamanan informasi yang disampaikan berikut ini harus disebutkan dalam kebijakan pengelolaan insiden keamanan informasi dan skema terkait.

- **Perlindungan data yang cukup dan privasi informasi pribadi yang tersedia**. Pada umumnya ada perundang-undangan yang spesifik yang mencakup kerahasiaan dan integritas data, sering dibatasi pada kendali data pribadi. Karena insiden keamanan informasi umumnya dihubungkan dengan individu, maka informasi yang bersifat pribadi perlu direkam dan dikelola. Suatu pendekatan terstruktur pada pengelolaan insiden keamanan informasi oleh karenanya perlu mempertimbangkan perlindungan privasi yang sesuai. Hal ini bisa meliputi:
  - individu dengan akses kepada data pribadi tidak boleh mengetahui orang yang diselidiki secara pribadi, sepanjang dapat dilaksanakan;
  - perjanjian kerahasiaan (*non-disclosure agreement*) harus ditandatangani oleh individu yang memiliki akses kepada data pribadi sebelum mereka diberikan akses untuk itu;
  - informasi hanya digunakan untuk keperluan yang dinyatakan , yaitu, untuk penyelidikan insiden keamanan informasi.

- **Tata kearsipan yang terpelihara.** Perusahaan diwajbkan memelihara arsip tentang kegiatan mereka untuk peninjauan ulang pada proses audit organisasi tahunan. Persyaratan serupa ada pada organisasi pemerintah. Organisasi diminta untuk melaporkan atau membuat arsip untuk penerapan hukum (misalnya kasus yang melibatkan kejahatan yang serius atau penetrasi kepada sistem pemerintah yang sensitif).

- **Perlindungan untuk memastikan pemenuhan kewajiban kontrak komersial**. Jika ada persyaratan mengikat tentang ketentuan layanan pengelolaan insiden keamanan informasi, misalnya mencakup waktu tanggapan yang diperlukan, suatu organisasi harus memastikan bahwa keamanan informasi yang sesuai, diberikan untuk menjamin bahwa kewajiban tersebut dapat dipenuhi dalam semua keadaan. (Terkait dengan ini, jika suatu organisasi mengontrak pihak luar untuk dukungan (lihat butir 7.5.4), misalnya CERT, maka harus dipastikan bahwa semua persyaratan, termasuk waktu tanggapan, dimasukkan dalam kontrak dengan pihak luar tersebut.)

- **Isu hukum yang terkait dengan kebijakan dan prosedur**. Kebijakan dan prosedur yang terkait dengan skema pengelolaan insiden keamanan informasi harus diperiksa potensi isu hukum dan regulasinya, misalnya, jika ada pernyataan tentang tindakan kedisiplinan dan/atau hukum yang diambil terhadap mereka yang menyebabkan insiden.

- **Penolakan diperiksa untuk kebenaran hukum**. Semua penolakan mengenai tindakan yang diambil oleh tim pengelolaan insiden informasi, dan personil pendukung eksternal, harus diperiksa kebenaran hukumnya.

- **Kontrak dengan personil pendukung eksternal mencakup semua aspek yang diperlukan**. Kontrak dengan personil pendukung eksternal, misalnya dari CERT, harus diperiksa secara menyeluruh menyangkut surat pelepasan tuntutan atas kewajiban, kerahasiaan, ketersediaan layanan, dan implikasi dari panduan yang salah.

- **Perjanjian kerahasiaan harus dapat diterapkan**. Anggota tim pengelolaan insiden keamanan informasi bisa diminta untuk menandatangani perjanjian kerahasiaan ketika memulai dan mengakhiri pekerjaan.

- **Persyaratan penerapan hukum harus dijelaskan**. Isu yang terkait dengan kemungkinan instansi penerapan hukum meminta informasi dari suatu skema pengelolaan insiden keamanan informasi harus jelas. Kejelasan diperlukan pada tingkatan minimum yang diperlukan oleh hukum dimana insiden harus didokumentasikan, dan berapa lama dokumentasi itu harus disimpan.

- **Aspek kewajiban harus jelas**. Isu kewajiban yang berpotensi muncul, dan perlindungan terkait yang diperlukan perlu diperjelas. Contoh dari kejadian yang berhubungan dengan isu kewajiban adalah:
  - jika suatu insiden bisa mempengaruhi organisasi lain sebagai contoh, penyingkapan informasi bagi-pakai (*shared information*), dan tidak diberitahukan pada waktunya dan organisasi yang lain mengalami dampak yang kurang baik,
  - jika ditemukan kerentanan baru dalam suatu produk, dan pemasok tidak diberitahu dan suatu insiden besar terkait kemudian terjadi dampak yang besar pada satu atau lebih organisasi yang lain,
  - suatu laporan tidak dibuat jika organisasi diharuskan untuk melaporkan atau membuat arsip mengenai kasus yang bisa melibatkan kejahatan yang serius, atau penetrasi ke dalam sistem pemerintah yang sensitif atau bagian dari infrastruktur nasional yang vital,
  - informasi yang diungkapkan menunjukkan bahwa seseorang, atau suatu organisasi, mungkin terlibat dalam suatu penyerangan. Hal ini dapat merusak reputasi dan bisnis dari orang atau organisasi yang terlibat.
  - informasi yang diungkapkan bahwa mungkin ada masalah dengan bagian tertentu dari perangkat lunak dan ini ternyata tidak benar.

- **Persyaratan regulasi yang spesifik harus dijelaskan**. Jika diperlukan oleh persyaratan regulasi yang spesifik, insiden harus dilaporkan kepada badan yang ditunjuk, sebagai contoh seperti yang dipersyaratkan dalam industri tenaga nuklir.

- **Tuntutan atau prosedur kedisiplinan internal harus berhasil.** Perlindungan keamanan informasi yang sesuai harus ada, mencakup jejak audit yang terbukti tidak dapat dirusak, agar dapat menuntut, atau membawa prosedur kedisiplinan internal terhadap 'penyerang', baik serangan teknis maupun fisik. Untuk mendukung ini, bukti biasanya dikumpulkan dengan cara yang dapat diterima oleh pengadilan atau forum kedisiplinan lainnya. Bukti harus dapat menunjukkan bahwa:
  - arsip lengkap dan belum dirusak dengan cara apapun,
  - salinan bukti elektronik dapat dibuktikan serupa dengan yang asli,
  - sistem TI menjadi sumber dari bukti yang dikumpulkan beroperasi dengan benar pada saat bukti dicatat.

- **Aspek hukum yang terkait dengan teknik pemantauan harus dijelaskan**. Implikasi penggunaan teknik pemantauan perlu diperhatikan dalam konteks perundang-undangan yang relevan. Faktor yang perlu dipertimbangkan meliputi siapa/apa yang dipantau, bagaimana ia dipantau, dan kapan pemantauan terjadi. Perlu juga dicatat bahwa pemantauan/pengintaian dalam konteks IDS (*Intrusion Detection System*) dibahas secara rinci dalam TR 18043.

- **Kebijakan penggunaan terdefinisi dan dikomunikasikan**. Penggunaan yang bisa diterima dalam organisasi harus didefinisikan, didokumentasikan dan dikomunikasikan ke semua pemakai. (Sebagai contoh, para pemakai harus diberitahu tentang kebijakan penggunaan yang bisa diterima dan diminta untuk memberikan pernyataan tertulis bahwa mereka memahami dan menerima kebijakan tersebut, ketika mereka bergabung dengan suatu organisasi atau diberi akses ke sistem informasi).

5.2.4 Efisiensi dan mutu operasional

Efisiensi dan mutu operasional dari suatu pendekatan terstruktur terhadap pengelolaan insiden keamanan informasi bersandar pada sejumlah faktor, termasuk kewajiban untuk memberitahukan tentang insiden, mutu pemberitahuan, kemudahan penggunaan, kecepatan dan pelatihan. Sebagian dari faktor-faktor ini berkaitan dengan usaha untuk memastikan bahwa pemakai menyadari tentang nilai dari pengelolaan insiden keamanan informasi dan dimotivasi untuk melaporkan insiden-insiden. Mengenai kecepatan, waktu yang diperlukan seseorang untuk melaporkan suatu insiden bukanlah satu-satunya faktor, tetapi juga waktu yang diperlukan untuk memproses data dan mendistribusikan informasi yang diproses (terutama dalam kasus siaga). Kesadaran dan program pelatihan yang sesuai harus dilengkapi dengan dukungan '*hot line*' dari personil pengelola insiden keamanan informasi, guna mengurangi penundaan.

5.2.5 Keadaan tanpa nama (*Anonymity*)

Isu keadaan tanpa nama adalah penting bagi keberhasilan pengelolaan insiden keamanan informasi. Pemakai harus diyakinkan bahwa sumbangan informasi mereka atas insiden keamanan informasi dilindungi sepenuhnya dan, bilamana perlu, dibersihkan sedemikian rupa sehingga tidak ada cara untuk mengaitkannya dengan organisasi mereka atau bagian daripadanya kecuali dengan persetujuan yang penuh.

Skema pengelolaan keamanan informasi harus memperhatikan situasi yang merupakan hal penting untuk memastikan keadaan tanpa nama dari seorang atau pihak yang melaporkan insiden keamanan informasi yang potensial dalam keadaan tertentu. Tiap organisasi harus mempunyai ketentuan yang menggambarkan dengan jelas ketentuan dari keadaan tanpa nama, atau kekurangan daripadanya, untuk orang atau pihak yang melaporkan suatu insiden keamanan informasi yang potensial. ISIRT mungkin perlu memperoleh informasi tambahan yang pada awalnya tergantung pada orang atau pihak yang melaporkan insiden tersebut. Lagipula, informasi penting tentang insiden keamanan informasi sendiri dapat diperoleh dari orang yang pertama kali mendeteksinya.

5.2.6 Kerahasiaan

Skema pengelolaan insiden keamanan informasi bisa memuat informasi yang sensitif, dan orang-orang yang terlibat dalam menangani insiden, diperlukan untuk menangani informasi yang sensitif. Selama mengolah informasi ini, proses ini harus di “anonimkan” atau personil dengan akses pada informasi ini disyaratkan menandatangani perjanjian kerahasiaan. Jika insiden keamanan informasi dicatat (*logged*) melalui sistem pengelolaan masalah umum, rinciannya bisa juga dihilangkan.

Sebagai tambahan, skema pengelolaan insiden keamanan informasi harus mempunyai ketentuan untuk mengendalikan komunikasi insiden kepada pihak luar, yang meliputi media, mitra bisnis, pelanggan, organisasi hukum, dan masyarakat.

5.2.7 Operasi yang terpercaya

Tim pengelola insiden keamanan informasi harus mampu secara efisien memenuhi kebutuhan fungsional, keuangan, hukum dan politik dari sebuah organisasi dan mampu menjalankan kebijakan organisasi ketika mengelola insiden keamanan informasi. Fungsi dari tim pengelola insiden keamanan informasi harus dapat diaudit secara bebas untuk mengkonfirmasikan bahwa semua persyaratan bisnis dipenuhi secara efektif. Lebih lanjut, cara yang baik untuk mencapai aspek kebebasan lainnya adalah dengan memisahkan rantai pelaporan tanggapan insiden dari jalur pengelola operasional dan membuat manajer senior bertanggung jawab langsung terhadap pengelolaan tanggapan insiden. Keuangan dari kapabilitas ini harus dipisahkan juga untuk menghindari pengaruh yang tidak baik.

5.2.8 Tipologi

Tipologi umum yang mencerminkan struktur umum pendekatan pengelolaan insiden keamanan informasi, akan menjadi salah satu faktor kunci untuk memberikan hasil yang konsisten. Tipologi, bersama-sama dengan metrik umum dan struktur basis data standar, akan menyediakan kapabilitas untuk membandingkan hasil, meningkatkan informasi siaga dan memungkinkan pandangan yang lebih akurat terhadap ancaman dan kelemahan sistem informasi[3].

CATATAN 3 Dokumen ini tidak mendefinisikan tipologi umum

6 Contoh insiden keamanan informasi dan penyebabnya

Insiden keamanan informasi bisa disengaja atau merupakan kecelakaan (misalnya disebabkan oleh kesalahan atau kejadian alam), dan bisa disebabkan oleh masalah teknis ataupun peralatan. Konsekuensinya meliputi insiden seperti penyingkapan atau modifikasi informasi dengan cara yang tidak sah, dirusak atau dibuat tidak tersedia, atau aset organisasi dirusak atau dicuri. Insiden keamanan informasi meliputi juga yang tidak dilaporkan, tidak ditetapkan sebagai insiden, tidak bisa diselidiki, atau tidak bisa dilindungi untuk mencegah pengulangan kembali.

Uraian tentang contoh insiden keamanan informasi serta penyebabnya di bawah ini, diberikan *sebagai ilustrasi saja*. Penting dicatat bahwa contoh ini bukanlah daftar contoh yang lengkap.

6.1 Penolakan layanan

Penolakan layanan (*Denial of Service* - DoS) adalah kategori umum dari suatu insiden. Insiden seperti ini menyebabkan sistem, layanan atau jaringan gagal beroperasi dalam kapasitas yang diharapkan, sering kali merupakan penolakan sepenuhnya terhadap akses dari pemakai yang sah.

Ada dua jenis insiden DoS yang disebabkan oleh hal teknis: penghapusan sumber daya (*resource elimination*) dan kurangnya sumber daya (*resource starvation*).
Beberapa contoh yang khas insiden DoS teknis yang sengaja meliputi:

- *"ping"* ke alamat jaringan *broadcast* agar memenuhi lebar pita (*bandwidth*) jaringan dengan lalu lintas tanggapan,

---

[3] Bukan tujuan dokumen ini untuk mendefinisikan tipologi umum. Pembaca dinasehatkan untuk mengacu kepada sumber alternatif untuk informasi tersebut.

- pengiriman data dalam suatu format yang tak diharapkan kepada sistem, layanan atau jaringan dalam usaha untuk menghentikan, atau mengganggu operasi normalnya,
- membuka banyak sesi pada sistem, layanan atau jaringan tertentu dalam usaha untuk menghabiskan sumber daya (yaitu dengan memperlambat, mengunci atau menghentikan).

Beberapa insiden DoS teknis bisa terjadi karena tidak disengaja, misalnya disebabkan oleh konfigurasi yang tidak benar dilakukan oleh operator atau tidak kompatibelnya perangkat lunak aplikasi, tetapi yang lain mungkin disengaja. Beberapa insiden DoS sengaja diluncurkan guna menghentikan suatu sistem, layanan, atau jaringan, sedang yang lainnya hanyalah produk sampingan dari kegiatan perusakan yang lain. Sebagai contoh, beberapa pemindaian (*scanning*) terselubung yang umum dan teknik identifikasi dapat menyebabkan sistem atau layanan yang sudah usang atau salah konfigurasi menjadi berhenti ketika dipindai. Harus dicatat bahwa banyak insiden DoS teknis yang disengaja sering dieksekusi dengan tanpa nama (yaitusumber serangan adalah 'palsu'), karena mereka secara tipikal tidak tergantung pada penerimaan kembali oleh penyerang informasi dari jaringan atau sistem yang diserang.

Insiden DoS yang disebabkan oleh hal non teknis, yang menyebabkan hilangnya informasi, layanan dan/atau fasilitas, bisa disebabkan, misalnya oleh:

- pelanggaran atas regulasi keamanan fisik yang menyebabkan terjadinya pencurian atau kerusakan yang disengaja dan perusakan peralatan,
- kerusakan perangkat keras yang tidak disengaja (dan/atau lokasinya) oleh api atau banjir,
- kondisi lingkungan yang ekstrim, misalnya suhu operasi yang tinggi (misal karena kerusakan pendingin udara),
- Sistem malfungsi atau kelebihan beban,
- perubahan sistem yang tidak terkendali,
- Malfungsi perangkat lunak atau perangkat keras.

6.2 Pengumpulan informasi

Pada dasarnya, kategori insiden pengumpulan informasi meliputi kegiatan-kegiatan yang dikaitkan dengan pengidentifikasian target potensial dan pemahaman layanan yang berjalan pada target tersebut. Jenis insiden ini dilakukan dengan pengintaian, dengan sasaran melakukan identifikasi terhadap:

- keberadaan suatu target, memahami topologi jaringan disekitarnya, dan dengan siapa target berkomunikasi secara rutin,
- kerentanan yang potensial pada target atau lingkungan jaringan terdekatnya yang bisa dimanfaatkan.

Contoh khas tentang penyerangan pengumpulan informasi secara teknis meliputi:

- pembuangan entri dari *Domain Name System* (DNS) – Sistem Nama Domain pada Internet Domain dari target (*zone transfer* DNS),
- *ping* ke alamat jaringan untuk mendapatkan informasi sistem yang aktif,
- menyelidiki sistem untuk mengidentifikasi (misal sidik jari) sistem operasi *host*,
- penelusuran *port* jaringan yang tersedia pada suatu sistem untuk mengidentifikasi layanan yang terkait (misal e-mail, FTP, Web, dll) dan versi perangkat lunak dari layanan tersebut,
- penelusuran satu atau lebih layanan yang rentan pada seluruh rangkaian alamat jaringan (telusuran horisontal).

Pada beberapa kasus, pengumpulan informasi teknis dapat juga menjadi kegiatan akses yang tidak sah, misalnya, sebagai bagian dari pencarian kerentanan sistem, penyerang juga

mencoba untuk memperoleh akses yang tidak sah. Ini biasanya terjadi dengan perangkat *hacking* otomatis yang tidak hanya mencari kerentanan tetapi juga secara otomatis mencoba mengeksploitasi kerentanan sistem, layanan dan/atau jaringan lemah yang ditemukan.

Insiden pengumpulan informasi yang disebabkan oleh hal non-teknis, menghasilkan:

- penyingkapan atau modifikasi secara langsung atau tidak langsung terhadap informasi,
- pencurian HAKI yang tersimpan secara elektronik,
- pelanggaran atas akuntabilitas, misal dalam *account logging* ,
- penyalahgunaan sistem informasi (misal bertentangan dengan hukum atau kebijakan organisasi),

bisa disebabkan, misalnya, oleh:

- pelanggaran regulasi keamanan fisik yang menghasilkan akses tidak sah kepada informasi, dan pencurian peralatan penyimpan data yang berisi data penting, misalnya kunci enkripsi,
- sistem operasi yang buruk atau salah konfigurasi karena perubahan sistem yang tidak terkendali, atau malfungsi perangkat lunak atau perangkat keras, yang menyebabkan personil internal atau eksternal yang tidak mempunyai otoritas memperoleh akses kepada informasi.

6.3 Akses yang tidak sah

Kategori insiden ini meliputi yang tidak termasuk dalam kedua kategori di atas. Umumnya kategori insiden ini terdiri dari usaha tidak sah untuk mengakses atau menyalahgunakan suatu sistem, layanan atau jaringan. Beberapa contoh insiden akses tidak sah yang distimulasi secara teknis meliputi:

- mencoba untuk mendapat berkas kata kunci (*password*),
- serangan luapan penyangga (*buffer overflow*) untuk mencoba untuk memperoleh akses istimewa (misal pengurus/administrator sistem) terhadap target,
- eksploitasi kerentanan protokol dengan tujuan membajak atau mengarahkan ke jurusan yang salah dari koneksi jaringan yang sah,
- berusaha menaikkan tingkat akses ke sumber daya atau informasi melebihi apa yang telah dimiliki dengan sah oleh administrator.

Insiden akses tidak sah yang disebabkan oleh hal non-teknis, menghasilkan penyingkapan atau modifikasi terhadap informasi secara langsung atau tidak langsung, pelanggaran akuntabilitas atau pengunaan yang salah dari sistem informasi, bisa disebabkan, misalnya oleh:

- pelanggaran terhadap regulasi keamanan fisik yang mengakibatkan akses tidak sah kepada informasi,
- sistem operasi yang kurang baik dan/atau salah konfigurasi karena perubahan sistem yang tidak terkendali, atau malfungsi perangkat lunak atau perangkat keras, dengan hasil yang serupa seperti yang diuraikan dalam butir 6.2 di atas.

7 Perencanaan dan persiapan

Tahap persiapan dan perencanaan pengelolaan insiden keamanan informasi memfokuskan pada:

- pendokumentasian insiden keamanan informasi, kebijakan pelaporan dan penanganannya, serta skema terkait (termasuk prosedur yang terkait),
- mendapatkan personil dan struktur organisasi pengelolaan insiden yang siap bekerja,
- melembagakan program pengarahan dan pelatihan kesadaran.

Dengan selesainya tahapan ini, suatu organisasi harus siap sepenuhnya untuk mengelola insiden keamanan informasi dengan baik.

7.1 Ikhtisar

Agar skema pengelolaan insiden keamanan informasi menjadi efektif dan efisien dalam penggunaan operasional, sejumlah kegiatan persiapan harus diselesaikan setelah tahap perencanaan. Kegiatan persiapan ini meliputi:

- perumusan dan pembuatan kebijakan pengelolaan insiden keamanan informasi, dan memperoleh komitmen pengelola senior atas kebijakan tersebut (lihat juga butir 7.2 di bawah),
- definisi dan dokumentasi skema pengelolaan insiden keamanan informasi secara terperinci (lihat juga butir 7.3 di bawah). Topik yang akan dimasukkan meliputi:
  - skala kerusakan dari insiden keamanan informasi yang akan digunakan untuk memeringkat insiden. Sebagaimana disebut dalam butir 4.2.1, skala ini bisa menjadi mayor dan minor, dengan keputusan yang didasarkan pada dampak buruk yang aktual atau yang diproyeksikan pada operasi bisnis organisasi,
  - formulir[4] pelaporan insiden[5] dan kejadian[6] keamanan informasi (contoh formulir seperti ditunjukkan dalam Lampiran A), tindakan dan prosedur yang didokumentasikan terkait dengan prosedur normal untuk penggunaan data dan cadangan (*back-up*) sistem, layanan dan/atau jaringan, serta rencana kesinambungan bisnis,
  - prosedur operasi untuk ISIRT, dengan tanggung-jawab yang didokumentasikan, dan alokasi peran untuk orang[7] yang ditunjuk untuk melakukan berbagai kegiatan, misalnya, termasuk:
    - mematikan sistem, layanan dan/atau jaringan yang terkena, yang dalam keadaan tertentu telah disepakati oleh regulasi sebelumnya dengan pengelola bisnis dan/atau TI yang relevan,
    - membiarkan sistem, layanan dan/atau jaringan yang terpengaruh tetap dihubungkan dan dijalankan,
    - memantau data yang mengalir dari, ke dan dalam suatu sistem yang terkena,
    - mengaktifkan cadangan dan prosedur perencanaan bisnis berkesinambungan dan tindakan yang sejalan dengan kebijakan keamanan terhadap sistem, layanan dan/atau jaringan,
    - pemantauan dan pemeliharaan pelestarian yang aman dari bukti elektronik, jika diperlukan untuk penuntutan atau tindakan kedisiplinan internal,
    - mengkomunikasikan rincian insiden keamanan informasi kepada orang atau organisasi internal dan eksternal,

- menguji penggunaan dari skema pengelolaan insiden keamanan informasi, proses dan prosedurnya (lihat juga butir 7.3.5 di bawah),
- pemuktahiran dari keamanan informasi perusahaan dan analisis risiko serta kebijakan manajemen, dan kebijakan keamanan informasi jaringan dan layanan, meliputi acuan kepada pengelolaan insiden keamanan informasi, dan memastikan bahwa kebijakan ini ditinjau secara teratur (lihat juga butir 7.4 di bawah),

---

[4] Jika memungkinkan semua formulir harus formulir elektronik (mis. dalam halaman web yang aman) dengan hubungan kepada database kejadian/insiden keamanan informasi. Dalam dunia masa kini, untuk mengoperasikan suatu skema berbasis kertas akan memakan waktu dan bukan cara operasi yang paling efisien.)

[5] Format digunakan oleh personil pengelolaan insiden keamanan informasi untuk membangun informasi yang dilaporkan pada inawalnya tentang kejadian keamanan informasi dan menyimpan catatan yang berjalan sampai penilaian insiden diselesaikan. Pada tiap tahap pembaharuan dimasukkan dalam database kejadian/insiden. Formulis catatan database kejadian/insiden keamananan informasi yang ‘diisi’ kemudian digunakan dalam kegiatan penyelesaian pasca insiden.

[6] Formulir diisi oleh personil pelaporan (bukan anggota timmm pengelolaan insiden keamanan informasi.

[7] Untuk organisasi yang lebih kecil, seseorang bisa diberi alokasi lebih dari satu peran.

- pembentukan ISIRT, dengan program pelatihan yang tepat yang dirancang, dikembangkan dan disediakan untuk personilnya (lihat juga butir 7.5 di bawah),
- sarana teknis dan lainnya untuk mendukung skema pengelolaan insiden keamanan informasi (dan dengan begitu pekerjaan ISIRT) (lihat juga butir 7.6 di bawah),
- rancangan dan pengembangan program kesadaran pengelolaan insiden keamanan informasi (lihat juga butir 7.7 di bawah), yang diikuti oleh penyerahannya kepada semua personil dari suatu organisasi (dan diulang ketika terjadi pergantian personil).

butir yang berikut menguraikan masing-masing kegiatan ini, termasuk isi tiap dokumen yang diperlukan.

7.2 Kebijakan pengelolaan insiden keamanan informasi

7.2.1 Maksud/tujuan

Kebijakan pengelolaan insiden keamanan informasi ditujukan kepada tiap orang yang memiliki akses yang sah kepada suatu sistem informasi dari organisasi dan lokasi terkait.

7.2.2 Audiens

Kebijakan pengelolaan insiden keamanan informasi harus disetujui oleh eksekutif senior suatu organisasi, dengan komitmen yang didokumentasikan dan dikonfirmasikan oleh semua pengelola senior. Kebijakan tersebut haruslah tersedia bagi tiap-tiap karyawan dan pemborong, dan harus disampaikan dalam pengarahan dan pelatihan kesadaran keamanan informasi (lihat juga butir 7.7 di bawah).

7.2.3 Isi

Isi kebijakan pengelolaan insiden keamanan informasi harus menangani topik yang berikut:

- pentingnya pengelolaan insiden keamanan informasi bagi organisasi, dan komitmen pengelola senior kepadanya dan skema terkait,
- ikhtisar pendeteksian kejadian keamanan informasi, pelaporan dan pengumpulan informasi yang relevan, dan bagaimana informasi ini harus digunakan untuk menentukan insiden keamanan informasi. Ikhtisar ini harus meliputi suatu ringkasan mengenai jenis insiden keamanan informasi yang mungkin, bagaimana melaporkannya, apa yang harus dilaporkan, di mana dan untuk siapa, dan termasuk bagaimana cara menangani seluruh jenis baru insiden keamanan informasi,
- ikhtisar penilaian insiden keamanan informasi, termasuk ringkasan siapa yang bertanggung jawab, apa yang harus dilakukan, pemberitahuan, dan eskalasi,
- ringkasan kegiatan yang mengikuti konfirmasi bahwa kejadian keamanan informasi adalah suatu insiden keamanan informasi. Ini harus meliputi:
  - tanggapan segera,
  - analisis forensik,
  - komunikasi kepada personil yang terlibat dan pihak ketiga yang relevan,
  - pertimbangan apakah suatu insiden keamanan informasi berada dibawah kendali,
  - tanggapan kemudian,
  - dorongan ‘krisis’,
  - kriteria eskalasi,
  - siapa yang bertanggung jawab.
- acuan kepada kebutuhan untuk memastikan bahwa semua kegiatan dicatat/*logged* dengan baik untuk analisis kemudian, dan dilakukan pemantauan berlanjut untuk memastikan pelestarian yang aman terhadap bukti elektronik, jika diperlukan untuk penuntutan hukum atau tindakan kedisiplinan internal,

- pasca kegiatan resolusi insiden keamanan informasi, termasuk pelajaran dari proses dan perbaikannya, mengikuti insiden keamanan informasi,
- rincian di mana dokumentasi rencana, termasuk prosedurnya, disimpan,

- tinjauan ISIRT terdiri dari topik berikut:
  - struktur organisasi ISIRT, dan identitas personil kunci, termasuk siapa yang bertanggung jawab atas:
    - pengarahan singkat pengelola senior tentang insiden,
    - menangani permintaan keterangan, mendorong kelanjutan, dll.,
    - hubungan dengan organisasi eksternal (jika perlu).
  - piagam pengelolaan keamanan informasi yang menetapkan apa yang akan dikerjakan ISIRT dan di bawah otoritas siapa melakukannya. Sedikitnya, piagam harus meliputi pernyataan misi, definisi lingkup ISIRT, dan rincian dari sponsor pimpinan terhadap ISIRT serta otoritasnya,
  - pernyataan misi ISIRT yang memfokuskan pada kegiatan inti tim. Agar dipertimbangkan, tim ISIRT harus mendukung penilaian, tanggapan, dan pengelolaan insiden keamanan informasi, untuk penyelesaian yang berhasil. Sasaran dan tujuan tim sangat penting, dan memerlukan definisi yang jelas, dan tidak rancu,
  - definisi lingkup kegiatan ISIRT. Secara normal, lingkup ISIRT suatu organisasi akan meliputi semua sistem, layanan dan jaringan informasi organisasi. Dalam kasus lain, karena alasan apapun, bisa membutuhkan lingkup yang kurang dari itu, dalam hal ini ia harus didokumentasikan dengan jelas apa yang termasuk dan yang tidak termasuk dalam lingkup,
  - Identitas dari pejabat eksekutif senior/anggota direksi/pengelola senior sponsor, yang memberi otoritas tindakan ISIRT, dan tingkat otoritas yang diberikan dalam ISIRT. Pengetahuan ini akan membantu semua personil organisasi untuk memahami latar belakang dan *set-up* ISIRT, dan merupakan informasi penting untuk membangun kepercayaan pada ISIRT. Harus dicatat bahwa rincian ini diumumkan, harus diperiksa terlebih dahulu dari perspektif hukum. Dalam beberapa keadaan, penyingkapan otoritas tim bisa digunakan untuk klaim kewajiban,
- ikhtisar dari kesadaran dan program pelatihan pengelolaan insiden keamanan informasi,
- ringkasan aspek hukum dan regulasi yang harus diperhatikan (lihat juga butir 5.2.3).

7.3 Skema pengelolaan insiden keamanan informasi

7.3.1 Maksud/tujuan

Tujuan dari skema pengelolaan insiden keamanan informasi adalah untuk menyediakan dokumentasi rinci yang menguraikan proses dan prosedur untuk menangani insiden dan untuk mengkomunikasikan insiden tersebut. Skema pengelolaan insiden keamanan informasi diberlakukan bilamana suatu kejadian keamanan informasi dideteksi. Skema ini digunakan sebagai pemandu untuk:

- menanggapi kejadian insiden keamanan informasi,
- menentukan apakah kejadian keamanan informasi menjadi insiden keamanan informasi,
- mengelola insiden keamanan informasi hingga dapat disimpulkan,
- mengidentifikasi pengalaman, dan perbaikan kepada skema dan/atau keamanan secara umum yang diperlukan,
- membuat perbaikan yang dapat diidentifikasikan.

7.3.2 Audiens

Skema pengelolaan insiden keamanan informasi dijelaskan kepada semua personil organisasi, dengan begitu mencakup mereka yang bertanggung jawab atas:

- pendeteksian dan pelaporan kejadian keamanan informasi oleh siapapun dalam organisasi, tenaga kontrak atau permanen,
- penilaian dan tanggapan atas kejadian keamanan informasi dan insiden keamanan informasi, dan dilibatkan pada pasca insiden tahap pemecahan pelajaran dan sebagaimana perlunya meningkatkan keamanan informasi dan skema pengelolaan insiden keamanan informasi itu sendiri. Ini meliputi anggota kelompok pendukung operasi (atau tim yang sejenis), ISIRT, pengelola, personil hubungan masyarakat dan wakil hukum.

Harus juga dipertimbangkan pemakai pihak ketiga, dan insiden keamanan informasi dan kerentanan terkait yang dilaporkan dari organisasi pihak ketiga, dan pemerintah serta insiden keamanan informasi komersial dan kerentanan ketentuan informasi organisasi.

7.3.3 Isi

Isi dokumentasi skema pengelolaan insiden keamanan informasi harus meliputi:

- ikhtisar kebijakan pengelolaan insiden keamanan informasi,
- ikhtisar skema pengelolaan insiden keamanan informasi secara keseluruhan,
- proses dan prosedur[8] yang terperinci, dan informasi tentang skala dan peralatan terkait, yang berhubungan dengan:
  - Perencanaan dan Persiapan:
    - pendeteksian dan pelaporan kejadian keamanan informasi (oleh manusia atau sarana otomatis),
    - pengumpulan informasi tentang kejadian keamanan informasi,
    - penilaian atas kejadian keamanan informasi (termasuk eskalasi sebagaimana diperlukan), menggunakan skala kerusakan kejadian/insiden yang disepakati, dan menentukan apakah kejadian-kejadian tersebut digolongkan kembali sebagai insiden keamanan informasi,
  - Penggunaan (jika insiden keamanan informasi telah ditetapkan):
    - pengkomunikasian keberadaan insiden keamanan informasi atau rinciannya yang relevan kepada organisasi atau orang internal dan eksternal,
    - sesuai dengan analisis dan penilaian skala kerusakan yang ditetapkan, pelembagaan tanggapan segera, yang dapat meliputi pengaktifan prosedur pemulihan, dan/atau pengkomunikasian kepada personil relevan yang terlibat,
    - pelaksanaan analisis forensik, sebagaimana diperlukan dan relatif terhadap nilai skala kerusakan insiden keamanan informasi, dan merubah nilai skala sebagaimana diperlukan,
    - memutuskan apakah insiden keamanan informasi berada dibawah kendali,
    - pelembagaan tanggapan lebih lanjut yang diperlukan, termasuk yang mungkin diperlukan kemudian (misalnya, dalam memudahkan pemulihan sepenuhnya dari suatu bencana,
    - jika insiden keamanan informasi tidak berada dibawah kendali, dorongan kegiatan 'krisis' (misalnya, pemanggilan pemadam kebakaran, atau mengaktifkan rencana kesinambungan bisnis),
    - eskalasi penilaian dan/atau keputusan lebih lanjut sebagaimana diperlukan,memastikan bahwa semua kegiatan dicatat dengan benar, untuk analisis lanjutan,pemutakhiran basis data kejadian/insiden keamanan informasi,

(Dokumentasi skema pengelolaan insiden keamanan informasi harus memungkinkan tanggapan insiden keamanan informasi segera dan dalam jangka waktu yang lebih lama. Semua insiden keamanan informasi akan memerlukan penilaian awal dari dampak buruk yang potensial, untuk jangka pendek dan panjang (sebagai contoh,

[8] Organisasi dapat memutuskan apakah semua prosedur dimasukkan dalam dokumentasiskem, atau semua atau sebagian dirindi dalam dokumen tambahan.

bencana besar bisa terjadi setelah suatu insiden keamanan informasi awal). Lebih lanjut, beberapa tanggapan mungkin perlu untuk insiden keamanan informasi yang tak terduga, dimana perlindungan sementara diperlukan. Bahkan pada situasi ini, dokumentasi skema ini harus meliputi panduan umum pada langkah-langkah yang mungkin perlu).

- Tinjauan:
  - pelaksanaan analisis forensik lebih lanjut, sebagaimana diperlukan,
  - pengidentifikasian dan pendokumentasian pengalaman dari insiden keamanan informasi,
  - peninjauan ulang dan pengidentifikasian perbaikan keamanan informasi, sebagai hasil dari pengalaman,
  - peninjauan ulang seberapa efektif proses dan prosedur dalam menanggapi, penilaian dan pemulihan tiap insiden keamanan informasi, dan pengidentifikasian perbaikan skema pengelolaan insiden keamanan informasi secara keseluruhan, sebagai hasil pengalaman,
  - pemutakhiran basis data kejadian/insiden keamanan informasi,

- Perbaikan-berdasarkan pengalaman, membuat perbaikan atas:
  - hasil analisis dan pengelolaan resiko keamanan informasi,
  - skema pengelolaan insiden keamanan informasi (sebagai contoh, proses dan prosedur, formulir pelaporan dan/atau struktur organisasi),
  - keamanan menyeluruh, dengan pelaksanaan perlindungan baru dan/atau yang diperbaiki.

- rincian skala kerusakan kejadian/insiden (misalnya, mayor atau minor, atau signifikan, mendesak, kecil, tidak mendesak) dan panduan terkait,
- pedoman untuk memutuskan apakah eskalasi diperlukan selama tiap proses yang relevan, dan untuk siapa, dan prosedur terkait. Seseorang yang menilai suatu kejadian atau insiden keamanan informasi harus menyadari, berdasarkan pedoman yang diberikan dalam dokumentasi skema pengelolaan insiden keamanan informasi, bila dalam keadaan normal diperlukan untuk mengeskalasi hal-hal, dan untuk siapa. Sebagai tambahan, akan ada keadaan yang tidak diketahui pada saat hal ini diperlukan. Misalnya, suatu insiden keamanan informasi minor bisa meningkat menjadi situasi signifikan atau 'krisis' jika tidak ditangani dengan baik atau insiden keamanan informasi minor tidak diatasi dalam seminggu bisa menjadi insiden keamanan informasi mayor. Pedoman harus mendefinisikan jenis kejadian dan insiden keamanan informasi, jenis eskalasi dan siapa yang dapat memulai eskalasi,
- prosedur yang harus diikuti untuk memastikan bahwa semua kegiatan dicatat dengan baik dalam bentuk yang sesuai, dan analisis terhadap catatan dilakukan oleh personil yang ditunjuk,
- prosedur dan mekanisme untuk memastikan bahwa perubahan rezim kendali dipelihara mencakup penjejakan/tracking insiden dan kejadian keamanan informasi dan pemutakhiran laporan insiden keamanan informasi, dan pemutakhiran skema itu sendiri,
- prosedur untuk analisis forensik,
- prosedur dan pedoman tentang penggunaan *Intrusion Detection Sistem* (IDS), untuk memastikan aspek-aspek hukum dan regulasi telah ditangani (lihat butir 5.2.3). Pedoman harus meliputi pembahasan dari keuntungan dan kerugian melakukan kegiatan pengintaian atas penyerang. Informasi lebih lanjut tentang IDS terdapat dalam ISO/IEC TR 15947-TI Intrusion Detection Framework, dan ISO/IEC TR 18043-Guidelines for the Selection, Deployment and Operation of Intrusion Detection Sistem (IDS),
- skema struktur organisasi,
- kerangka acuan dan tanggung-jawab dari ISIRT secara keseluruhan, dan masing-masing anggota,
- informasi kontak yang penting.

7.3.4 Prosedur

Sebelum mampu memulai operasi skema pengelolaan insiden keamanan informasi, adalah penting bahwa prosedur yang terdokumentasikan, telah diperiksa, dan telah tersedia. Tiap dokumen prosedur harus menunjukkan siapa yang bertanggung jawab atas penggunaan dan pengelolaannya, yang sesuai dari kelompok pendukung operasi dan/atau ISIRT. Prosedur seperti itu akan meliputi mereka yang akan memastikan bahwa bukti elektronik dikumpulkan dan disimpan dengan aman, dan pelestariannya yang aman dipantau secara berkesinambungan, jika diperlukan dalam penuntutan hukum atau tindakan kedisiplinan internal. Lebih lanjut, harus ada prosedur yang didokumentasikan yang mencakup tidak hanya kelompok pendukung operasi dan kegiatan ISIRT, tetapi mereka yang terlibat dalam analisis forensik dan kegiatan 'krisis' - jika tidak tercakup di tempat lain (misalnya dalam rencana kesinambungan bisnis). Sesungguhnya prosedur yang didokumentasikan harus seluruhnya sejalan dengan kebijakan pengelolaan insiden keamanan informasi yang didokumentasikan dan dokumentasi skema pengelolaan insiden keamanan informasi lain.

Adalah penting memahami bahwa tidak semua prosedur harus tersedia bagi umum. Misalnya, tidak diinginkan seluruh personil organisasi untuk memahami operasi internal ISIRT untuk saling berhubungan dengannya. ISIRT harus memastikan bahwa pedoman yang 'tersedia untuk umum', meliputi informasi yang merupakan hasil analisis insiden keamanan informasi, adalah dalam bentuk yang tersedia, sebagai contoh tentang Intranet organisasi. Lagipula, mungkin juga penting menyimpan beberapa rincian skema pengelolaan insiden keamanan informasi dengan ketat untuk mencegah "orang dalam" merusak proses penyelidikan. Sebagai contoh, jika seorang karyawan bank yang menggelapkan dana mengetahui beberapa rincian skema, ia mungkin lebih baik menyembunyikan kegiatan mereka dari penyelidik atau jika tidak menghambat pendeteksian dan penyelidikan dari pemulihan suatu insiden keamanan informasi.

Isi prosedur operasi akan tergantung pada sejumlah kriteria, terutama yang berhubungan dengan bentuk insiden dan kejadian keamanan informasi potensial yang diketahui dan jenis asset sistem informasi yang terlibat serta lingkungannya. Jadi, suatu prosedur operasi bisa dihubungkan dengan jenis tertentu insiden atau tentu saja dengan jenis produk (sebagai contoh *firewalls*, basis data, sistem operasi, aplikasi) atau produk yang spesifik. Tiap prosedur operasi harus dengan jelas mengidentifikasi langkah-langkah yang akan diambil dan siapa yang akan mengerjakannya. Prosedur harus mencerminkan pengalaman dari luar (misalnya pemerintah dan CERT komersil atau yang serupa, dan para pemasok) serta dari sumber internal.

Akan ada prosedur operasi untuk menangani jenis kejadian keamanan informasi dan insiden keamanan informasi yang telah diketahui. Harus ada juga prosedur operasi yang harus diikuti ketika kejadian keamanan informasi atau insiden keamanan informasi bukan dari jenis yang dikenal. Dalam hal ini yang berikut perlu diperhatikan:

- proses pelaporan untuk penanganan seperti 'pengecualian',
- pedoman tentang pemilihan waktu untuk mendapatkan persetujuan dari pengelola guna menghindari penundaan tanggapan,
- pendelegasian pra-otorisasi tentang pengambilan keputusan tanpa proses persetujuan yang normal.

7.3.5 Skema pengujian

Pemeriksaan dan pengujian berkala proses dan pengelolaan insiden keamanan informasi dan prosedur harus dijjadwalkan untuk menyoroti permasalahan dan kekurangan potensial yang mungkin timbul selama pengelolaan kejadian keamanan informasi dan insiden keamanan informasi. Setiap perubahan yang timbul setelah tinjauan tanggapan harus dikenakan pengujian dan pemeriksaan yang seksama sebelum berfungsi.

7.4 Keamanan informasi dan kebijakan pengelolaan resiko

7.4.1 Maksud/tujuan

Maksud/tujuan memasukkan isi pengelolaan insiden keamanan informasi dalam kebijakan pengelolaan resiko dan kebijakan keamanan informasi perusahaan, dan kebijakan keamanan sistem, layanan dan jaringan informasi spesifik, adalah untuk:

- menjelaskan mengapa pengelolaan insiden keamanan informasi, khususnya skema penanganan dan pelaporan insiden keamanan informasi, adalah penting,
- menunjukkan komitmen pengelola senior terhadap perlunya penyiapan dan tanggapan yang sesuai terhadap insiden keamanan informasi, yaitu kepada skema pengelolaan insiden keamanan informasi,
- memastikan konsistensi berbagai kebijakan,
- memastikan tanggapan terencana, sistematis dan wajar terhadap insiden keamanan informasi, sehingga memperkecil dampak insiden yang buruk,

7.4.2 Isi

Keamanan informasi perusahaan dan kebijakan pengelolaan resiko, dan kebijakan keamanan sistem, layanan atau jaringan informasi spesifik, harus dimutakhirkan sehingga secara tegas mengacu kepada kebijakan pengelolaan insiden keamanan informasi dan skema terkait. Bagian yang relevan harus mengacu kepada komitmen pengelola senior, dan menguraikan secara singkat:

- kebijakan,
- proses skema, dan infrastruktur yang terkait,
- persyaratan pendeteksian, pelaporan, penilaian dan pengelolaan insiden,

dan menunjukkan dengan jelas personil yang bertanggung jawab untuk mengizinkan dan/atau melakukan tindakan kritis tertentu (misalnya memutuskan sistem informasi atau bahkan mematikannya).

Selanjutnya, kebijakan membutuhkan mekanisme tinjauan yang sesuai dibentuk untuk memastikan bahwa setiap informasi dari pendeteksian, pamantauan dan resolusi insiden keamanan informasi digunakan sebagai masukan untuk memastikan kelanjutan efektivitas keamanan informasi perusahaan dan pengelolaan resiko, kebijakan sistem yang spesifik, keamanan jaringan layanan informasi.

7.5 Pembentukan ISIRT

7.5.1 Maksud/tujuan

Maksud/tujuan pembentukan ISIRT adalah untuk memberikan kepada organisasi personil yang sesuai untuk menilai, menanggapi dan belajar dari insiden keamanan informasi, serta menyediakan koordinasi, pengelolaan, umpan balik dan komunikasi yang perlu. ISIRT dapat memberikan sumbangan atas pengurangan kerusakan fisik dan moneter, serta pengurangan kerusakan atas reputasi organisasi yang kadang-kadang dihubungkan dengan insiden keamanan informasi.

7.5.2 Anggota dan struktur

Ukuran, struktur dan komposisi ISIRT harus sesuai dengan struktur ukuran organisasi. Walaupun ISIRT bisa merupakan suatu tim atau bagian tersendiri, anggota boleh berbagi tugas-tugas lain, yang akan mendorong masukan dari anggota dari bidang-bidang lain dalam organisasi. Seperti dibahas dalam butir 4.2.1 dan 7.1, dalam banyak kesempatan ISIRT akan

merupakan suatu tim bayangan yang dipimpin oleh seorang manajer senior. Manajer senior akan didukung oleh individu yang mempunyai spesialisasi pada topik tertentu, misalnya dalam penanganan serangan kode yang jahat, yang akan dipanggil berdasarkan jenis insiden keamanan informasi terkait. Tergantung pada ukuran organisasi, seorang anggota boleh memegang lebih dari satu peran dalam ISIRT. ISIRT bisa juga terdiri dari individu dari bagian-bagian berbeda dari organisasi (misalnya Operasi Bisnis, TI/Telekomunikasi, Audit, SDM dan Pemasaran).

Anggota Tim harus dapat dihubungi, sehingga nama dan rincian kontak tiap anggota dan cadangannya harus tersedia dalam organisasi. Sebagai contoh, rincian yang perlu harus dengan jelas ditunjukkan dalam dokumentasi skema pengelolaan insiden keamanan informasi, yang mencakup dokumen prosedural, dan formulir pelaporan, tetapi bukan dalam pernyataan kebijakan.

Pengelola ISIRT harus:

- diberi wewenang untuk membuat keputusan segera tentang bagaimana menghadapi suatu insiden,
- umumnya memiliki jalur pelaporan khusus kepada pengelola senior, terpisah dari operasi bisnis normal,
- memastikan bahwa semua anggota ISIRT mempunyai pengetahuan dan keterampilan, dan ini akan terus dipelihara/dijaga,
- menugaskan penyelidikan tiap insiden kepada anggota yang paling sesuai dari timnya.

7.5.3 Hubungan dengan bagian-bagian lain organisasi

Pengelola ISIRT dan anggota timnya harus mempunyai tingkat otoritas untuk mengambil tindakan yang perlu yang dianggap sesuai sebagai tanggapan atas insiden keamanan informasi. Meskipun demikian, tindakan yang mungkin berdampak kurang baik atas organisasi secara keseluruhan, baik secara finansial maupun reputasi, harus disetujui oleh pengelola senior. Karena alasan itu, adalah penting untuk merinci kebijakan pengelolaan insiden keamanan informasi dan skema otoritas yang sesuai bagi pengelola ISIRT melaporkan insiden keamanan informasi yang serius.

Prosedur dan tanggung-jawab untuk berhubungan dengan media harus juga disetujui oleh pengelola senior dan didokumentasikan. Prosedur ini menetapkan:

- siapa dalam organisasi yang akan menangani pertanyaan media,
- bagaimana bagian organisasi akan saling berhubungan dengan ISIRT.

7.5.4 Hubungan dengan pihak eksternal

Hubungan antara ISIRT dan pihak eksternal yang sesuai perlu dibangun. Pihak eksternal bisa meliputi:

- personil pendukung eksternal yang dikontrak, misalnya dari CERT,
- ISIRT dari organisasi eksternal atau tim penanggap insiden komputer, atau CERT,
- organisasi penerapan hukum,
- otoritas darurat lainnya (misalnya pemadam kebakaran),
- organisasi pemerintah yang sesuai,
- personil hukum,
- pejabat hubungan masyarakat dan/atau anggota media,
- mitra bisnis,
- pelanggan,
- masyarakat.

7.6 Dukungan teknis dan lainnya

Tanggapan yang cepat dan efektif terhadap insiden keamanan informasi akan lebih mudah dicapai jika semua saran atas dukungan teknis yang perlu dan dukungan lainnya telah diperoleh, disiapkan dan diuji. Hal ini meliputi:

- akses ke rincian asset organisasi (terutama dengan daftar asset terbaru) dan informasi tentang hubungannya dengan fungsi bisnis,
- akses kepada strategi kesinambungan bisnis yang terdokumentasikan dan rencana yang terkait,
- proses komunikasi yang diumumkan dan didokumentasikan
- penggunaan basis data elektronik dari kejadian/insiden keamanan informasi dan sarana teknis untuk mengisi dan memutakhirkan basis data dengan cepat, menganalisis informasi dan memudahkan tanggapan (walaupun diketahui bahwa adakalanya ada kejadian dimana catatan manual masih tetap diperlukan atau digunakan oleh suatu organisasi),
- regulasi kesinambungan bisnis yang memadai untuk basis data kejadian/insiden keamanan informasi.

Sarana teknis yang digunakan untuk mengisi dan memutakhirkan basis data dengan cepat, menganalisis informasinya dan memudahkan tanggapan terhadap insiden keamanan informasi harus mendukung:

- penguasaan cepat kejadian keamanan dan laporan insiden informasi,
- pemberitahuan personil yang dipilih sebelumnya (sebagai orang eksternal yang relevan) dengan sarana yang sesuai (misalnya surat elektronik, fax, telepon, dll.), dengan begitu memerlukan pemeliharaan basis data kontak yang dapat dipercaya (yang harus siap diakses, dan harus meliputi catatan/kertas dan pendukung lainnya), dan fasilitas untuk menyampaikan informasi kepada individu dengan cara yang aman bilamana diperlukan,
- pengambilan tindakan pencegahan yang setaraf dengan resiko yang dinilai untuk memastikan bahwa komunikasi elektronik, apakah internet atau non internet, tidak bisa disadap (*eavesdropped*) selagi sistem, layanan dan/atau jaringan sedang diserang,
- pengambilan tindakan pencegahan yang setaraf dengan resiko yang dinilai untuk memastikan bahwa komunikasi elektronik, apakah internet atau non internet, tersedia selagi sistem, layanan dan/atau jaringan sedang diserang,
- memastikan pengumpulan semua data tentang sistem informasi, layanan dan/atau jaringan, dan semua data yang diproses,
- jika setaraf dengan resiko yang dinilai, pengendalian integritas kriptografi digunakan untuk membantu menentukan apakah dan bagian-bagian mana dari sistem, layanan dan/atau jaringan, dan data apa, yang telah diubah,
- memudahkan pengarsipan dan pengamanan informasi yang dikumpulkan (sebagai contoh, dengan memberikan tandatangan digital pada buku catatan dan bukti lain sebelum penyimpanan *off-line* dalam media *read-only* seperti CD atau DVD ROM),
- memungkinkan persiapan dari hasil cetakan komputer (misalnya dari buku catatan), termasuk mereka yang menunjukkan kemajuan suatu insiden, dan proses penyelesaian dan rantai penjagaan,
- pemulihan sistem informasi, layanan dan/atau jaringan kepada operasi normal, dengan:
  - prosedur membuat cadangan yang baik,
  - cadangan yang bersih dan handal,
  - pengujian cadangan,
  - kendali kode yang jahat (*malicious code*),
  - media asli dengan sistem dan perangkat lunak aplikasi,
  - media yang bisa dipakai untuk proses *boot*,
  - sistem dan tambahan aplikasi yang bersih, terbaru dan handal

  sejalan dengan rencana kesinambungan bisnis yang relevan.

Suatu sistem, layanan dan jaringan informasi yang diserang, tidak akan berfungsi dengan benar. Jadi, sejauh mungkin, dan setaraf dengan resiko yang dinilai, tidak ada sarana teknis (perangkat lunak dan keras) yang perlu untuk menanggapi suatu insiden keamanan informasi yang harus diandalkan dalam operasinya pada sistem 'utama', layanan dan/atau jaringan organisasi. Jika memungkinkan, mereka harus mandiri sepenuhnya.

Semua sarana teknis harus dipilih dengan hati-hati, diterapkan dengan benar dan secara teratur diuji (termasuk pengujian cadangan yang dibuat).

Harus dicatat bahwa sarana teknis yang diuraikan dalam butir ini tidak mencakup sarana teknis yang digunakan secara langsung untuk mendeteksi insiden keamanan informasi dan penyusupan dan secara otomatis memberitahu orang yang sesuai. Sarana teknis tersebut diuraikan dalam *Intrusion Detection Framework TR 15947* dan dalam *Management of information and communication technology security (MICTS)* TR 13335, terutama sekali Bagian 2.

7.7 Kesadaran dan pelatihan

Pengelolaan insiden keamanan informasi adalah proses yang melibatkan tidak hanya sarana teknis tetapi juga orang-orang, dan dengan begitu harus didukung oleh individu terlatih sadar keamanan informasi dalam organisasi.

Kesadaran dan partisipasi dari semua personil organisasi sangat penting untuk keberhasilan pendekatan pengelolaan insiden keamanan informasi yang terstruktur. Karena alasan ini, peran pengelola insiden keamanan informasi perlu dipromosikan secara aktif sebagai bagian dari kesadaran keamanan informasi perusahaan dan program pelatihan. Program kesadaran dan material yang terkait harus tersedia bagi semua personil, termasuk karyawan baru dan, jika relevan, pemakai dan kontraktor pihak ketiga. Harus ada program pelatihan spesifik untuk kelompok pendukung operasi, anggota ISIRT, dan, jika diperlukan, personil keamanan informasi dan administrator yang spesifik. Harus dicatat bahwa tiap kelompok orang yang terlibat langsung dengan pengelolaan insiden memerlukan tingkat pelatihan yang berbeda, tergantung pada jenis, frekuensi dan kekritisan interaksi mereka dengan skema pengelolaan insiden keamanan informasi.

Pengarahan singkat kesadaran harus meliputi:

- dasar tentang bagaimana skema pengelolaan insiden keamanan informasi bekerja, termasuk ruang lingkupnya dan keamanan kejadian dan insiden pengelolaan 'aliran kerja',
- bagaimana cara melaporkan tentang kejadian dan insiden keamanan informasi,
- bila relevan, perlindungan kerahasiaan dari sumber,
- perjanjian tingkat layanan dari skema,
- pemberitahuan hasil - di bawah keadaan apa sumber akan disarankan,
- batasan yang dikenakan oleh perjanjian kerahasiaan,
- otoritas organisasi pengelolaan insiden keamanan informasi dan jalur pelaporannya,
- siapa dan bagaimana menerima laporan dari skema pengelolaan insiden keamanan informasi.

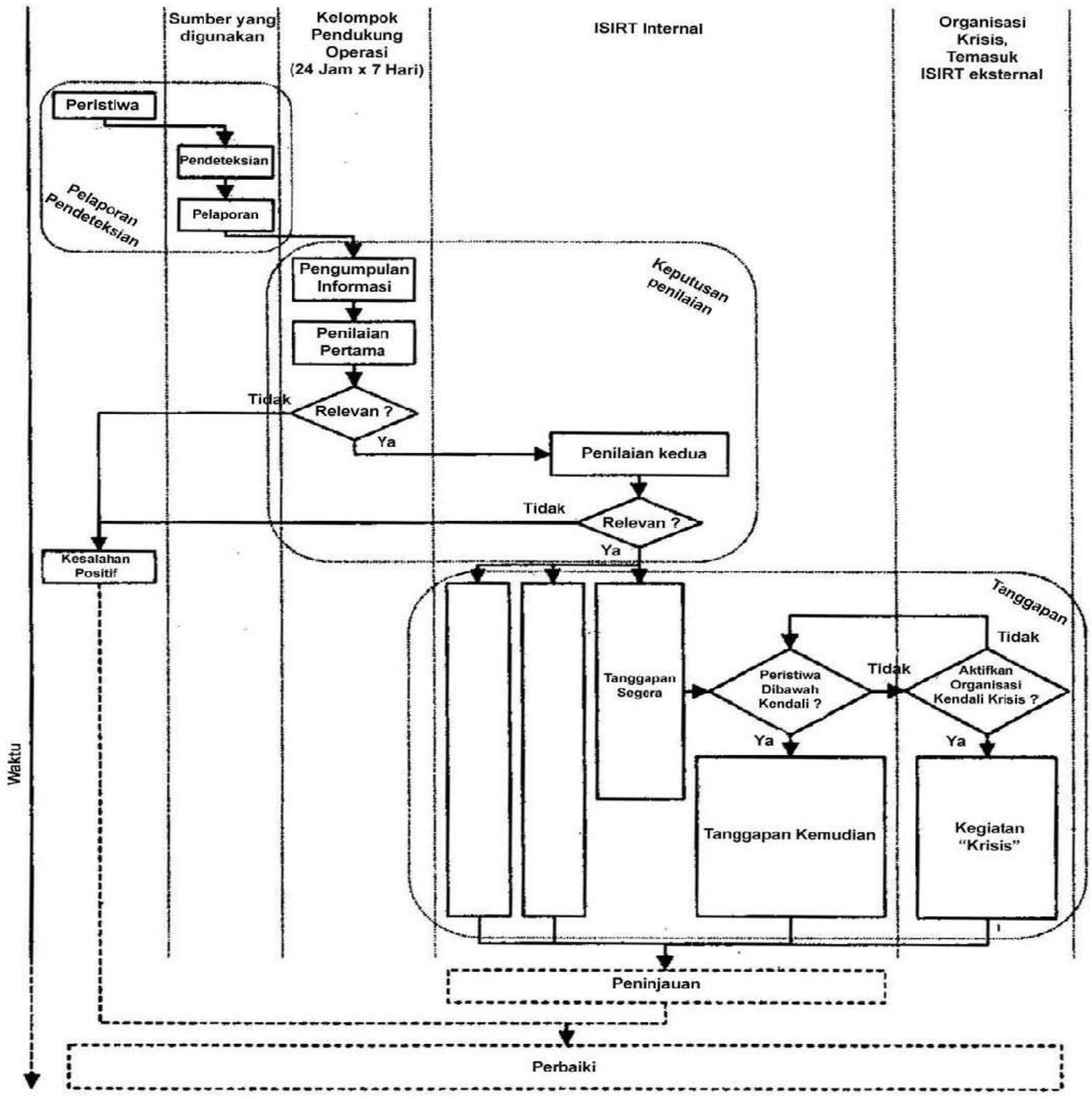
Dalam beberapa hal mungkin saja diinginkan secara khusus memasukkan rincian kesadaran tentang pengelolaan insiden keamanan informasi dalam program pelatihan lainnya (sebagai contoh, program orientasi personil atau program kesadaran keamanan perusahaan secara umum). Pendekatan kesadaran ini bisa memberikan konteks berharga yang relevan kepada kelompok orang tertentu, dan dapat meningkatkan efektivitas dan efisiensi program pelatihan.

Sebelum skema pengelolaan insiden keamanan informasi menjadi operasional, semua personil yang relevan perlu terbiasa dengan prosedur yang terlibat dalam pendeteksian dan pelaporan kejadian keamanan informasi, dan personil yang terpilih harus memahami tentang proses berikutnya. Ini harus diikuti dengan pengarahan dan latihan secara berkala. Pelatihan harus didukung oleh latihan spesifik dan pengujian untuk kelompok pendukung operasi dan anggota ISIRT, dan personil keamanan informasi dan pengurus yang spesifik.

8 Penggunaan

8.1 Pendahuluan

Pengelolaan insiden keamaan informasi dalam operasi meliputi dua fasa-utama, "Penggunaan" dan "Peninjauan Ulang", dan ini diikuti 'Perbaikan" jika perbaikan diketahui sebagai hasil dari pengalaman. Tahap ini dan proses yang terkait telah disampaikan dalam butir 4.2. Tahap “Penggunaan” diuraikan dalam butir ini, "Peninjauan Ulang": dalam butir 9, dan "Perbaikan" diuraikan dalam butir 10.
Ketiga tahap, dan proses yang terkait, ditunjukkan dalam Gambar 2 di bawah.



Gambar 2 – Diagram Alir Kejadian dan Insiden Keamanan Informasi

8.2 Ikhtisar dari proses-proses kunci

Dalam tahap Penggunaan, proses kunci adalah:

- pendeteksian dan pelaporan terjadinya kejadian keamanan informasi, baik oleh salah satu personil/konsumen organisasi atau secara otomatis (misalnya, dengan suatu peringatan dari *firewall*),
- pengumpulan informasi tentang kejadian keamanan informasi, dan melakukan penilaian awal oleh personil[9] kelompok pendukung operasi organisasi, yang akan menentukan apakah kejadian tersebut adalah suatu insiden keamanan informasi atau alarm palsu,
- melakukan penilaian kedua oleh ISIRT, untuk pertama-tama mengkonfirmasikan bahwa kejadian adalah suatu insiden keamanan informasi, dan kemudian, mendorong tanggapan segera serta mulai analisis forensik yang perlu, dan kegiatan komunikasi,
- Peninjauan ulang oleh ISIRT untuk menentukan jika insiden keamanan informasi berada dibawah kendali, dan:
  - jika ya, mendorong permintaan kemudian, lebih lanjut, tanggapan, dan memastikan semua informasi siap untuk kegiatan peninjauan ulang pasca insiden,
  - jika tidak, mendorong kegiatan 'krisis' dan melibatkan personil yang terkait, misalnya manajer dan tim kesinambungan bisnis organisasi,
- eskalasi, atau suatu dasar yang diperlukan sepanjang tahapan, untuk penilaian dan/atau keputusan lebih jauh,
- memastikan bahwa semua yang terlibat, terutama sekali ISIRT, mencatat semua kegiatan untuk analisis kemudian dengan baik,
- memastikan bahwa bukti elektronik dikumpulkan dan disimpan dengan aman, dan pemeliharaannya secara berkesinambungan terus dipantau, jika diperlukan untuk penuntutan hukum atau tindakan kedisiplinan internal,
- memastikan bahwa perubahan rezim kendali dipelihara yang mencakup penjejakan insiden keamanan informasi dan pemutakhiran laporan insiden, dan dengan demikian basis data kejadian/insiden keamanan informasi termutakhirkan.

Semua informasi yang dikumpulkan yang menyangkut kejadian atau insiden keamanan informasi harus disimpan dalam basis data kejadian/insiden keamanan informasi yang dikelola oleh ISIRT. Informasi yang dilaporkan di tiap proses harus selengkap mungkin seperti adanya pada waktu itu, untuk memastikan tersedianya dasar yang kuat untuk penilaian dan pembuatan keputusan, dan tentu saja tindakan yang diambil.

Sekali kejadian keamanan informasi dideteksi dan dilaporkan, tujuan proses berikutnya adalah:

- pendistribusian tanggung jawab untuk kegiatan pengelolaan insiden melalui hirarki personil yang sesuai, dengan penilaian, pengambilan keputusan dan tindakan yang menyertakan keamanan dan personil non-keamanan,
- menyediakan prosedur formal kepada tiap orang yang diberitahu untuk diikuti, termasuk peninjauan ulang dan perbaikan laporan yang dibuat, penilaian, dan pemberitahuan personil yang relevan (dengan tindakan individu tergantung pada jenis dan kesulitan insiden),
- penggunaan panduan untuk pendokumentasian yang lengkap dari kejadian keamanan informasi, dan bila kemudian kejadian tersebut digolongkan sebagai insiden keamanan informasi, tindakan yang berikutnya, adalah pemutakhiran basis data kejadian/insiden keamanan informasi.

Panduan tentang:

- pendeteksian insiden keamanan informasi dan pelaporan dijelaskan dalam butir 8.3,

---

[9] Secara normal tidak diharapkan personil kelompok pendukung operasi adalah tenaga ahli keamanan.

- penilaian dan keputusan (seperti apakah suatu insiden keamanan informasi digolongkan sebagai suatu insiden keamanan informasi) dijelaskan dalam butir 8.4,
- tanggapan terhadap insiden keamanan informasi dijelaskan dalam butir 8.5, yang mencakup:
  - tanggapan yang segera,
  - peninjauan ulang untuk menentukan jika suatu insiden keamanan informasi berada dibawah kendali,
  - tanggapan kemudian,
  - kegiatan 'krisis',
  - analisis forensik,
  - komunikasi,
  - komentar tentang isu eskalasi,
  - kegiatan pencatatan

8.3 Pendeteksian dan pelaporan

Kejadian keamanan informasi bisa dideteksi langsung oleh seseorang atau orang-orang yang memberitahukan sesuatu yang menyebabkan kekhawatiran, apakah terkait dengan masalah teknis, fisik atau prosedural. Pendeteksian misalnya, dapat dari pendeteksi asap/api atau alarm pencuri, dengan peringatan yang diberitahukan ke lokasi yang telah ditentukan untuk diambil tindakan. Kejadian keamanan informasi teknis bisa dideteksi oleh sarana otomatis - sebagai contoh, peringatan dibuat oleh fasilitas analisis jejak audit, *firewalls*, IDS, dan perangkat lunak anti virus, pada setiap kasus dipicu oleh parameter yang diatur sebelumnya.

Apapun sumber pendeteksian kejadian keamanan informasi, orang yang diberitahu oleh alat otomatis, atau secara langsung melihat sesuatu yang tidak biasa, bertanggung jawab untuk memulai pendeteksian dan proses pelaporan. Orang tersebut bisa dari anggota suatu organisasi, baik personil permanen atau dikontrak. Orang tersebut harus mengikuti prosedur dan menggunakan formulir pelaporan kejadian keamanan informasi yang ditetapkan oleh skema pengelolaan insiden keamanan informasi, untuk kejadian keamanan informasi menjadi perhatian kelompok pendukung dan pengelola operasi. Jadi, adalah penting bahwa semua personil menyadari dengan baik, dan mempunyai akses kepada panduan untuk pelaporan berbagai jenis kejadian keamanan informasi yang mungkin, termasuk format pelaporan kejadian keamanan informasi, dan rincian personil yang harus diberitahu tentang tiap kejadian. (Adalah masuk akal bahwa semua personil sedikitnya sadar akan format pelaporan insiden keamanan informasi, untuk membantu pemahaman mereka tentang skema tesebut.)

Bagaimana suatu kejadian keamanan informasi yang ditangani akan tergantung pada jenis kejadiannya, dan implikasi serta akibat yang ditimbulkan dari kejadian tersebut. Bagi banyak orang, ini akan merupakan keputusan di luar wewenang mereka. Jadi, orang yang melaporkan suatu kejadian keamanan informasi harus mengisi formulir pelaporan kejadian keamanan informasi dengan sebanyak mungkin narasi dan informasi lain yang tersedia pada saat itu, bertindak sebagai penghubung dengan manajer lokal sebagaimana diperlukan. Formulir tersebut, lebih disukai dalam format elektronik (misalnya dalam bentuk e-mail atau web), harus dikomunikasikan dengan aman kepada kelompok pendukung yang ditunjuk (yang harus menyediakan layanan 24 jam dan 7 hari seminggu), dengan suatu salinan kepada manajer ISIRT. Suatu contoh dari formulir pelaporan kejadian keamanan informasi dijelaskan dalam Lampiran A.

Perlu ditekankan bahwa tidak hanya ketelitian tetapi juga ketepatan waktu adalah penting dalam pengisian formulir pelaporan kejadian keamanan informasi. Bukanlah praktek yang baik dengan menunda penyerahan formulir pelaporan untuk meningkatkan akurasi isi laporan. Jika pelapor tidak yakin atas isian data dalam formulir pelaporan, laporan harus

diserahkan dengan catatan yang sesuai, dan perbaikan dikomunikasikan kemudian. Harus juga diketahui bahwa beberapa mekanisme pelaporan elektronik (misalnya e-mail) merupakan target penyerangan.

Ketika ada permasalahan, atau dianggap ada, dengan mekanisme pelaporan elektronik *baku* (misalnya e-mail), termasuk ketika dianggap sistem sedang diserang dan formulir pelaporan dapat dibaca oleh orang yang tidak berhak, maka harus menggunakan sarana komunikasi alternatif. Sarana alternatif bisa meliputi orang, telepon atau pesan teks. Sarana alternatif itu harus digunakan terutama sekali jika pada awal penyelidikan suatu kejadian keamanan informasi nampaknya dapat digolongkan sebagai suatu insiden keamanan informasi, terutama sekali yang dianggap signifikan.

Harus dicatat bahwa selagi dalam banyak kasus kejadian keamanan informasi harus dilaporkan untuk tindakan yang dilakukan oleh kelompok pendukung operasi, ada kemungkinan dimana suatu kejadian keamanan informasi dapat ditangani secara lokal. Suatu kejadian keamanan informasi mungkin dengan cepat dapat ditentukan sebagai alarm palsu, atau mungkin saja diselesaikan hingga diperoleh kesimpulan yang memuaskan. Dalam kasus seperti itu formulir pelaporan harus diisi dan diserahkan kepada pengelola lokal, dan kepada kelompok pendukung operasi dan kepada ISIRT untuk keperluan pencatatan, yaitu. ke dalam basis data kejadian/insiden keamanan informasi. Dalam keadaan tersebut, orang yang melaporkan penyingkapan kejadian keamanan informasi dapat mengisikan beberapa informasi yang diperlukan untuk formulir pelaporan kejadian keamanan informasi - jika demikian adanya maka formulir pelaporan insiden keamanan informasi harus juga diisi dan disampaikan.

8.4 Penilaian dan keputusan kejadian/insiden

8.4.1 Penilaian pertama dan keputusan awal

Orang yang menerima laporan dalam kelompok pendukung operasi harus menyatakan penerimaan formulir pelaporan kejadian keamanan informasi yang telah diisi, dan memasukkannya ke dalam basis data kejadian/insiden keamanan informasi, dan meninjau ulang laporan tersebut. Ia harus mendapatkan klarifikasi dari orang yang melaporkan kejadian keamanan informasi tersebut, dan mengumpulkan informasi lebih lanjut yang diperlukan dan diketahui tersedia, baik dari pelapor maupun dari tempat lain. Kemudian, kelompok pendukung operasi harus melakukan penilaian untuk menentukan apakah kejadian keamanan informasi harus digolongkan sebagai suatu insiden keamanan informasi atau alarm palsu. Jika kejadian keamanan informasi adalah alarm palsu, formulir pelaporan kejadian keamanan informasi harus dilengkapi dan dikomunikasikan kepada ISIRT untuk ditambahkan ke basis data dan tinjauan keamanan informasi, dan salinannya diberikan kepada pelapor dan manajer lokalnya.

Informasi dan bukti lain yang dikumpulkan pada tahap ini mungkin perlu digunakan di masa depan untuk tindakan kedisiplinan atau proses hukum. Orang atau orang-orang yang melakukan pengumpulan dan tugas penilaian informasi harus dilatih tentang persyaratan untuk pengumpulan dan pemeliharaan bukti.

Sebagai tambahan terhadap tanggal dan waktu tindakan, perlu mendokumentasikan secara lengkap:

- apa yang dilihat dan dikerjakan (termasuk alat yang digunakan) dan mengapa,
- lokasi 'bukti',
- bagaimana bukti diarsipkan (jika bisa),
- bagaimana memverifikasi bukti telah dilakukan (jika bisa),
- rincian penjagaan/penyimpanan material dan akses selanjutnya pada material tersebut.

Jika kejadian keamanan informasi ditentukan seperti layaknya suatu insiden keamanan informasi, dan kelompok pendukung operasi mempunyai tingkat kemampuan yang sesuai, penilaian lebih lanjut bisa dilakukan. Ini bisa mengakibatkan diperlukannya tindakan perbaikan segera, sebagai contoh dikenalinya tambahan perlindungan darurat dan ditunjuknya orang yang tepat untuk melakukan tindakan. Mungkin saja suatu kejadian keamanan informasi ditentukan sebagai insiden keamanan informasi yang signifikan (penggunaan skala kerusakan organisasi yang ditentukan sebelumnya), dalam hal mana manajer ISIRT harus diberitahu secara langsung. Mungkin saja situasi 'krisis' harus diumumkan, dan, sebagai contoh, manajer kesinambungan bisnis diberitahu untuk menjalankan rencana kesinambungan bisnis, serta manajer ISIRT dan pengelola senior juga harus diberitahu. Meskipun demikian, situasi yang paling mungkin terjadi adalah insiden keamanan informasi harus disampaikan langsung kepada ISIRT untuk penilaian dan tindakan lebih lanjut.

Apapun langkah berikutnya yang ditetapkan, anggota kelompok pendukung operasi harus mengisi selengkap mungkin formulir pelaporan insiden keamanan informasi. Suatu contoh formulir pelaporan insiden keamanan informasi disajikan dalam Lampiran A. Formulir pelaporan insiden keamanan informasi harus berisi narasi, dan sejauh mungkin harus mengkonfirmasikan dan menguraikan:

- apa insiden keamanan informasi itu,
- bagaimana terjadinya - dan oleh apa atau siapa,
- apa yang dipengaruhi atau dapat mempengaruhi,
- dampak atau dampak potensial dari insiden keamanan informasi atas bisnis organisasi,
- suatu indikasi apakah insiden keamanan informasi dianggap penting atau tidak (menggunakan skala kerusakan organisasi yang ditentukan sebelumnya),
- bagaimana penanganannya sejauh ini.

Ketika mempertimbangkan dampak buruk yang berpotensi muncul atau telah muncul dari suatu insiden keamanan informasi atas bisnis organisasi, yang disebabkan:

- penyingkapan informasi yang tidak sah,
- modifikasi informasi yang tidak sah,
- penyanggahan informasi,
- ketidaktersediaan informasi dan/atau layanan,
- perusakan informasi dan/atau layanan,

maka langkah pertama adalah mempertimbangkan konsekuensi-konsekuensi mana yang relevan.

Contoh kategori adalah:

- Kerugian finansial pada Operasi Bisnis,
- Minat Komersial dan Ekonomi,
- Informasi Pribadi,
- Kewajiban Hukum dan Regulasi,
- Pengelolaan dan Operasi Bisnis,
- Kehilangan Reputasi.

Untuk insiden yang dianggap relevan, panduan kategori yang terkait harus digunakan untuk menentukan dampak potensial atau nyata yang dapat dimasukkan ke dalam laporan insiden keamanan informasi. Contoh panduan disajikan dalam Lampiran B.

Jika suatu insiden keamanan informasi telah diselesaikan, laporan harus meliputi rincian perlindungan yang telah diambil dan pengalaman (misalnya perlindungan yang akan diadopsi untuk mencegah pengulangan kejadian atau kejadian yang serupa).

Setelah diisi selengkap mungkin, formulir pelaporan harus diserahkan kepada ISIRT untuk dimasukkan ke dalam basis data dan tinjauan kejadian/insiden keamanan informasi.
Jika suatu penyelidikan nampaknya lebih dari satu minggu, laporan sementara harus dibuat.

Harus ditekankan bahwa anggota kelompok pendukung operasi yang menilai suatu insiden keamanan informasi sadar, didasarkan pada panduan yang disajikan dalam dokumentasi skema pengelolaan insiden keamanan informasi:

- kapan perlu melakukan eskalasi dan kepada siapa,
- bahwa dalam semua kegiatan yang dilakukan oleh kelompok pendukung operasi, prosedur kendali perubahan yang didokumentasikan harus diikuti.

Jika ada masalah, atau dianggap ada masalah, dengan mekanisme pelaporan *baku* elektronik (misalnya e-mail), termasuk jika dianggap memungkinkan sistem sedang diserang dan formulir pelaporan bisa dibaca oleh orang yang tidak berhak, maka sarana alternatif pelaporan kepada manajer ISIRT harus digunakan. Sarana alternatif bisa meliputi orang, melalui telepon atau pesan teks. Sarana alternatif seperti itu harus digunakan terutama sekali ketika nampak bahwa suatu insiden keamanan informasi adalah signifikan.

8.4.2 Penilaian Kedua dan Konfirmasi Insiden

Penilaian kedua, dan konfirmasi atau keputusan apakah suatu kejadian keamanan informasi akan digolongkan sebagai suatu insiden keamanan informasi, merupakan tanggung jawab ISIRT. Personil ISIRT yang menerima harus:

- menyatakan penerimaan 'formulir pelaporan insiden keamanan informasi yang diisi selengkap mungkin oleh kelompok pendukung operasi,
- memasukkan formulir ke dalam basis data kejadian/insiden keamanan informasi,
- meminta klarifikasi dari kelompok pendukung operasi,
- meninjau ulang isi formulir pelaporan,
- mengumpulkan informasi lebih lanjut yang diperlukan dan diketahui tersedia, baik dari kelompok pendukung operasi, orang yang mengisi formulir pelaporan kejadian keamanan informasi atau dari lainnya.

Jika masih ada ketidakpastian yang menyangkut keaslian insiden keamanan informasi atau kelengkapan informasi yang dilaporkan, anggota ISIRT harus melakukan penilaian untuk menentukan apakah insiden keamanan informasi adalah benar atau hanya alarm palsu. Jika insiden keamanan informasi adalah suatu alarm palsu, laporan insiden keamanan informasi harus diisi, ditambahkan kepada basis data kejadian/insiden keamanan informasi dan dikomunikasikan kepada manajer ISIRT. Salinan laporan harus dikirim kepada kelompok pendukung operasi, dan pelapor serta manajer lokalnya.

Jika insiden keamanan informasi adalah benar, maka anggota ISIRT, dengan menyertakan rekan kerjanya sebagaimana diperlukan, harus melakukan penilaian lebih lanjut. Tujuannya adalah untuk mengkonfirmasikan secepat mungkin:

- apakah insiden keamanan informasi itu, bagaimana terjadinya – oleh apa atau siapa dan apa yang dipengaruhi atau dapat dipengaruhi, dampak atau dampak potensial insiden keamanan informasi pada bisnis organisasi, suatu indikasi apakah insiden keamanan informasi dianggap penting atau tidak (menggunakan skala kerusakan organisasi yang ditentukan sebelumnya),
- serangan teknis oleh seseorang yang disengaja atas sistem informasi, layanan dan/atau jaringan, sebagai contoh:
  - seberapa dalam sistem, layanan dan/atau jaringan telah diterobos, dan seberapa tinggi/level kendali yang dimiliki penyerang,
  - data apa yang telah diakses oleh penyerang, kemungkinan disalin, diubah atau dihancurkan,

  - perangkat lunak apa yang telah disalin, diubah atau dihancurkan oleh penyerang,
- serangan fisik oleh seseorang yang disengaja atas sistem informasi, layanan dan/atau perangkat keras jaringan dan/atau lokasi fisik, sebagai contoh:
  - apa pengaruh langsung atau tidak langsung dari kerusakan fisik (apakah keamanan akses fisik tidak ada?),
- untuk insiden keamanan informasi yang tidak langsung disebabkan oleh tindakan seseorang, pengaruh langsung atau tidak langsung (sebagai contoh, apakah akses fisik terbuka oleh karena api, apakah suatu sistem informasi lemah oleh karena malfungsi beberapa perangkat lunak atau jalur komunikasi, atau oleh karena kesalahan manusia),
- bagaimana insiden keamanan informasi telah ditangani sejauh ini.

Ketika meninjau ulang pengaruh buruk potensial atau aktual suatu insiden keamanan informasi pada bisnis suatu organisasi, dari:
- penyingkapan informasi yang tidak sah,
- modifikasi informasi yang tidak sah,
- penyanggahan informasi,
- tidak tersedianya informasi dan/atau layanan,
- penghancuran informasi dan/atau layanan,

akan diperlukan untuk mengkonfirmasikan konsekuensi mana yang relevan. Contoh kategori adalah:
- kerugian finansial atas Operasi Bisnis,
- minat Komersial dan Ekonomi,
- informasi Pribadi,
- kewajiban Hukum dan Regulasi
- pengelolaan dan Operasi Bisnis,
- kehilangan Kemauan.

Untuk yang dianggap relevan, kategori panduan yang terkait harus digunakan untuk membangun dampak potensial atau aktual untuk masuk ke dalam laporan insiden keamanan informasi. Contoh panduan dijelaskan dalam Lampiran B.

8.5 Tanggapan

8.5.1 Tanggapan segera

8.5.1.1 Ikhtisar

Pada sebagian besar kasus, kegiatan yang berikutnya untuk Anggota ISIRT adalah mengidentifikasi tindakan tanggapan yang segera untuk menangani insiden keamanan informasi, merekam rincian formulir insiden keamanan informasi, dan merekam dalam basis data kejadian/insiden keamanan informasi, dan memberitahukan tindakan yang diperlukan kepada orang atau kelompok yang tepat. Ini bisa mengakibatkan perlindungan darurat (sebagai contoh, mematikan sistem informasi, layanan dan/atau jaringan yang terpengaruh, dengan persetujuan lebih dulu dari pengelola TI dan/atau bisnis yang relevan), dan/atau pengidentifikasian perlindungan permanen tambahan, dan diberitahukan kepada orang atau kelompok yang sesuai. Jika belum dilakukan, pentingnya insiden keamanan informasi harus ditentukan, dengan penggunaan skala kerusakan organisasi yang ditetapkan terlebih dahulu, dan jika penting pengelola senior harus diberitahu secara langsung. Jika jelas situasi 'krisis' harus diumumkan, sebagai contoh manajer kesinambungan bisnis harus diberitahu mengenai kemungkinan pengaktifan rencana kesinambungan bisnis, dengan memberitahukan juga manajer ISIRT dan pengelola senior.

8.5.1.2 Tindakan Contoh

Sebagai suatu contoh dari tindakan tanggapan segera yang relevan dalam kasus serangan yang disengaja pada suatu sistem, layanan dan/atau jaringan informasi dapat dibiarkan tersambung ke Internet, atau jaringan yang lain, untuk:

- memungkinkan aplikasi bisnis yang kritis berfungsi dengan benar,
- mengumpulkan sebanyak mungkin informasi tentang penyerang,

dengan ketentuan bahwa penyerang tidak mengetahui bahwa ia sedang dalam pengawasan.

Meskipun demikian, selagi menjalankan keputusan tersebut, perlu dipertimbangkan faktor-faktor yang berikut:

- penyerang menyadari bahwa ia sedang diamati dan bisa melakukan tindakan yang akan menyebabkan kerusakan lebih jauh kepada sistem, layanan dan/atau jaringan informasi, dan data terkait,
- penyerang bisa menghancurkan informasi yang mungkin berguna untuk melacaknya.

Adalah penting bahwa secara teknis memungkinkan secara cepat dan handal untuk mematikan sistem, layanan dan/atau jaringan informasi yang diserang, bila telah diambil keputusan demikian. Meskipun demikian, sarana otentikasi yang sesuai harus diterapkan sehingga individu yang tidak berhak tidak bisa melakukan tindakan tersebut.

Pertimbangan lebih lanjut adalah pencegahan terulangnya kejadian tersebut yang biasanya merupakan prioritas tinggi, dan bisa disimpulkan dengan baik bahwa penyerang telah memaparkan suatu kelemahan yang harus diperbaiki, dan keuntungan dari pelacakannya tidak membenarkan usaha tersebut. Ini terutama sekali relevan jika penyerang tidak jahat dan telah menyebabkan sedikit kerusakan atau tidak sama sekali.

Berkaitan dengan insiden keamanan informasi yang disebabkan oleh sesuatu selain dari serangan yang disengaja, sumber tersebut harus diidentifikasikan. Mungkin perlu untuk mematikan sistem, layanan dan/atau jaringan informasi, atau mengisolasi bagian yang relevan dan mematikannya (dengan persetujuan lebih dulu dari pengelola TI dan/atau bisnis yang relevan), selagi perlindungan diterapkan. Ini mungkin mengambil waktu yang lebih panjang jika kelemahan adalah mendasar pada disain sistem informasi, layanan dan/atau jaringan, atau jika itu merupakan kelemahan yang kritis.

Kegiatan tanggapan lain mungkin mengaktifkan teknik pengawasan (sebagai contoh, '*honeypots*' - lihat TR 18043). Ini harus atas dasar prosedur yang didokumentasikan untuk skema pengelolaan insiden keamanan informasi.

Informasi yang mungkin dirusak oleh insiden keamanan informasi harus diperiksa oleh anggota ISIRT dengan membandingkannya dengan *cadangan* arsip untuk mengetahui terjadinya modifikasi, penghapusan, atau penyisipan informasi. Mungkin perlu memeriksa kesahihan catatan (*log*), karena penyerang yang sengaja mungkin telah memanipulasi catatan ini untuk menutupi jejaknya.

8.5.1.3 Pemutakhiran Informasi Insiden

Apapun langkah berikutnya yang ditetapkan, anggota ISIRT harus memutakhirkan laporan insiden keamanan informasi selengkap mungkin, menambahkannya kepada basis data kejadian/insiden keamanan informasi dan memberitahu pengelola ISIRT dan yang lain sebagaimana diperlukan. Pemutakhiran meliputi informasi lebih lanjut tentang:

- apakah insiden keamanan informasi,
- bagaimana disebabkannya - dan dengan apa atau siapa,
- apa yang dipengaruhinya atau dapat dipengaruhinya,

- dampak atau dampak potensial insiden keamanan informasi pada bisnis organisasi,
- perubahan kepada indikasi apakah insiden keamanan informasi dianggap penting atau tidak (menggunakan skala kerusakan organisasi yang ditetapkan lebih dahulu),
- bagaimana hal itu ditangani sejauh ini.

Jika suatu insiden keamanan informasi telah diselesaikan, laporan harus meliputi rincian perlindungan yang telah diambil dan pengalaman lain (misalnya perlindungan lebih lanjut yang akan diadopsi untuk mencegah pengulangan atau kejadian serupa). Laporan yang dimutakhirkan harus ditambahkan pada basis data kejadian/insiden keamanan informasi, dan diberitahukan kepada pengelola ISIRT dan pihak lain sebagaimana diperlukan.

Hal ini perlu ditekankan bahwa ISIRT bertanggung jawab untuk memastikan retensi yang aman dari semua informasi yang menyinggung insiden keamanan informasi untuk analisis lebih lanjut, dan penggunaan bukti hukum yang potensial. Sebagai contoh, untuk insiden keamanan informasi yang berorientasi pada TI, setelah penemuan awal insiden, semua data yang bersifat mudah hilang (*volatile*) harus dikumpulkan sebelum sistem, layanan dan/atau jaringan TI yang terpengaruh dimatikan, untuk penyelidikan forensik lengkap. Informasi yang dikumpulkan meliputi isi memori, *cache* dan *register*, dan rincian tentang segala proses yang berjalan, dan:

- duplikasi forensik yang lengkap atas sistem, layanan dan/atau jaringan yang terpengaruh, atau melakukan cadangan catatan tingkat rendah (*low level backup*) dan file yang penting harus diduplikasi tergantung pada sifat insiden keamanan informasi,
- catatan sistem, layanan dan jaringan yang berdekatan, sebagai contoh termasuk dari *router* dan *firewall*, harus dikumpulkan dan ditinjau,
- semua informasi yang dikumpulkan harus disimpan dengan aman pada media baca saja (*read-only*),
- dua atau lebih orang harus hadir ketika dilakukan duplikasi forensik, untuk menyatakan dan menerangkan bahwa semua kegiatan telah dilakukan sesuai dengan perundang-undangan dan peraturan yang relevan,
- spesifikasi dan uraian tentang alat dan perintah yang digunakan untuk melaksanakan duplikasi forensik harus didokumentasikan dan disimpan bersama-sama dengan media yang asli.

Anggota ISIRT akan juga bertanggung jawab, jika mungkin pada tahap ini, untuk memudahkan pengembalian fasilitas yang terpengaruh (apakah TI atau lainnya) ke status opersional yang aman yang tahan terhadap serangan yang sama.

8.5.1.4 Kegiatan lebih lanjut

Jika anggota ISIRT menentukan bahwa suatu insiden keamanan informasi adalah benar, maka kegiatan penting lainnya harus:

- memulai analisis forensik,
- menginformasikan kepada mereka yang bertanggung jawab atas komunikasi internal dan eksternal tentang fakta dan proposal yang harus dikomunikasikan, dalam bentuk apa dan untuk siapa.

Pada saat laporan insiden keamanan informasi telah diisi selengkapnya, maka laporan tersebut harus dimasukkan ke dalam basis data kejadian/insiden keamanan informasi dan dikomunikasikan kepada manajer ISIRT.

Jika suatu penyelidikan kemungkinan akan lebih dari waktu yang disetujui sebelumnya di dalam organisasi, maka laporan sementara harus dibuat. Anggota ISIRT yang menilai insiden keamanan informasi harus sadar, berdasarkan pada pedoman yang diberikan dalam dokumentasi skema pengelolaan insiden keamanan informasi:

- kapan mengeskalasi hal tersebut dan kepada siapa,
- bahwa dalam semua kegiatan yang diselenggarakan oleh ISIRT, prosedur kendali perubahan dokumentasi harus diikuti.

Jika ada permasalahan, atau dianggap ada, dengan fasilitas komunikasi yang normal (misalnya. e-mail), termasuk ketika dianggap mungkin sistem di bawah serangan, dan:

- disimpulkan bahwa insiden keamanan informasi adalah penting, dan/atau
- situasi 'krisis' telah ditentukan,

maka suatu insiden keamanan informasi harus pertama-tama dilaporkan secepatnya kepada orang-orang yang relevan langsung, melalui telepon atau pesan teks.

Bilamana dianggap perlu, pengelola ISIRT, dalam hubungan dengan pengelola keamanan informasi organisasi dan manajer senior/anggota dewan, harus bertindak sebagai penghubung dengan semua pihak terkait, internal dan eksternal kepada organisasi (lihat butir 7.5.3 dan 7.5.4).

Untuk memastikan bahwa hubungan tersebut diorganisasi dengan cepat dan efektif, maka perlu membuat metoda komunikasi sebelumnya, yang tidak sepenuhnya mengandalkan pada sistem, layanan dan/atau jaringan yang mungkin terpengaruh oleh insiden keamanan informasi. Regulasi ini bisa mencakup pencalonan dari penasehat cadangan atau wakilnya bila tidak hadir.

8.5.2 Insiden dibawah kendali

Setelah anggota ISIRT telah memulai tanggapan segera, dan seperti kegiatan komunikasi dan analisis forensik yang relevan, suatu pendapat harus segera dipastikan apakah insiden keamanan informasi berada dibawah kendali. Jika perlu, anggota ISIRT bisa membicarakannya dengan rekan kerja, pengelola ISIRT dan/atau orang atau kelompok lainnya.

Jika insiden keamanan informasi dikonfirmasikan dibawah kendali, maka anggota ISIRT harus membuat tanggapan kemudian yang diperlukan, dan analisis forensik dan komunikasi (lihat butir 8.5.3, 8.5.5 dan 8.5.6 di bawah), untuk menutup insiden keamanan informasi dan yang memulihkan sistem informasi yang terpengaruh kembali ke operasi normal.

Jika insiden keamanan informasi dikonfirmasikan tidak dibawah kendali, maka anggota ISIRT harus membuat 'kegiatan krisis" (lihat butir 8.5.4 di bawah).

8.5.3 Tanggapan kemudian

Setelah menentukan bahwa suatu insiden keamanan informasi berada dibawah kendali, dan tidak terkena kegiatan 'krisis', maka anggota ISIRT harus mengidentifikasi tanggapan selanjutnya yang diperlukan untuk menangani insiden keamanan informasi. Ini bisa meliputi pemulihan sistem, layanan dan/atau jaringan informasi yang terpengaruh kembali kepada operasi normal. Ia harus mencatat rincian formulir pelaporan insiden keamanan informasi dan dalam basis data kejadian/insiden keamanan informasi, dan memberitahukan mereka yang bertanggung jawab menyelesaikan tindakan terkait. Sekali tindakan ini telah diselesaikan, rinciannya harus dicatat dalam formulir pelaporan insiden keamanan informasi dan dalam basis data kejadian/insiden keamanan informasi, dan kemudian insiden keamanan informasi harus ditutup dan personil yang terkait diberitahu.

Beberapa tanggapan akan diarahkan kepada pencegahan pengulangan atau munculnya insiden keamanan informasi yang serupa. Sebagai contoh, jika ditentukan bahwa penyebab insiden keamanan informasi adalah kesalahan perangkat keras atau perangkat lunak TI,

tanpa tersedianya perbaikan (*patch*), maka pemasok harus dihubungi segera. Jika kerentanan TI yang diketahui menyebabkan insiden keamanan informasi ia harus diperbaiki dengan pemutakhiran keamanan informasi yang relevan. Setiap masalah yang terkait dengan konfigurasi TI yang perlu diperhatikan (*highlighted*) dalam insiden keamanan informasi harus ditangani. Tindakan lain untuk mengurangi kemungkinan pengulangan atau timbulnya kejadian yang serupa dari insiden keamanan informasi TI bisa meliputi perubahan sistem kata kunci dan menonaktifkan layanan yang tidak dipakai.

Bidang kegiatan tanggapan lain bisa melibatkan pemantauan sistem, layanan dan/atau jaringan TI. Mengikuti penilaian insiden keamanan informasi, mungkin tepat bila ada tambahan perlindungan pemantauan untuk membantu pendeteksian kejadian-kejadian yang tidak biasa dan mencurigakan yang merupakan gejala dari insiden keamanan informasi lebih lanjut. Pemantauan seperti itu bisa juga mengungkapkan secara lebih mendalam insiden keamanan informasi, dan mengidentifikasikan sistem TI lain yang dikompromikan.

Mungkin perlu pengaktifan tanggapan spesifik yang didokumentasikan dalam rencana kesinambungan bisnis yang relevan. Ini bisa berlaku untuk insiden keamanan informasi yang terkait dengan TI dan non TI. Tanggapan seperti itu harus termasuk semua aspek bisnis tidak hanya terkait secara langsung dengan TI tetapi juga pemeliharaan fungsi bisnis kunci dan kemudian pemulihan termasuk telekomunikasi suara, tingkatan personil dan fasilitas fisik.

Bidang kegiatan terakhir adalah pemulihan sistem, layanan dan/atau jaringan informasi yang terpengaruh pada operasi normal. Pemulihan sistem, layanan dan/atau jaringan informasi yang terpengaruh kepada keadaan operasional normal yang aman bisa dicapai melalui perbaikan tambahan (*patches*) untuk kerentanan yang dikenal dengan menonaktifkan unsur yang merupakan materi pokok yang dikompromikan. Jika karena kerusakan catatan selama insiden keamanan informasi, insiden keamanan informasi tidak diketahui, maka perlu pembangunan kembali sistem, layanan dan/atau jaringan informasi lengkap. Mungkin perlu pengaktifan bagian-bagian dari rencana kesinambungan bisnis yang relevan.

Jika suatu insiden keamanan informasi tidak terkait dengan TI, misalnya disebabkan oleh kebakaran, banjir atau bom, maka kegiatan pemulihan yang akan diikuti adalah yang terdokumentasikan dalam rencana kesinambungan bisnis yang relevan.

8.5.4 Kegiatan 'krisis'

Sebagaimana dibahas dalam butir 8.5.2, mungkin saja ketika ISIRT menentukan apakah insiden keamanan informasi berada dibawah kendali, kesimpulannya adalah bahwa ia tidak dibawah kendali dan perlu ditangani sebagai kegiatan 'krisis', menggunakan rencana yang ditentukan lebih dulu.

Pilihan terbaik untuk menangani semua jenis insiden keamanan informasi yang mungkin yang bisa mempengaruhi ketersediaan/kerusakan dan sampai tahap tertentu integritas sistem informasi, harus telah diidentifikasikan dalam strategi kesinambungan bisnis organisasi. Pilihan ini harus secara langsung dihubungkan dengan prioritas bisnis organisasi dan terkait dengan jadwal waktu pemulihan, dan dengan periode waktu maksimum yang dapat diterima akan putusnya TI, suara, manusia dan akomodasi. Strategi harus sudah mengidentifikasikan:

- tindakan pencegahan, kehandalan dan dukungan kesinambungan bisnis,
- struktur dan tanggung-jawab organisasi untuk pengelolaan perencanaan kesinambungan bisnis,
- struktur dan garis besar isi untuk rencana atau rencana-rencana kesinambungan bisnis.

Rencana kesinambungan bisnis, dan perlindungan yang ada untuk mendukung pengaktifan rencana itu, sekali diuji dengan memuaskan, maka akan membentuk basis untuk menangani kegiatan paling 'krisis', dimana kegiatan paling 'krisis' tersebut telah ditentukan.

Kemungkinan jenis lain dari kegiatan 'krisis' meliputi, tetapi tidak terbatas pada, pengaktifan:

- fasilitas pemadaman kebakaran dan prosedur evakuasi,
- fasilitas pencegahan banjir dan prosedur evakuasi,
- 'penanganan' bom dan prosedur evakuasi terkait,
- penyelidik spesialis penipuan sistem informasi,
- penyelidik spesialis serangan teknis.

8.5.5 Analisis forensik

Diidentifikasikan oleh penilaian lebih dulu sebagaimana diperlukan untuk tujuan pembuktian – *de facto* dalam konteks insiden keamanan informasi yang penting, analisis forensik harus dilakukan oleh ISIRT. Analisis forensik harus melibatkan penggunaan alat dan teknik penyelidikan berdasarkan TI, didukung oleh prosedur yang didokumentasikan, meninjau ulang insiden keamanan informasi yang ditunjuk secara lebih rinci dibanding dengan yang telah terjadi sampai sekarang dalam proses pengelolaan insiden keamanan informasi. Itu harus dilakukan secara terstruktur, dan, bila relevan, mengidentifikasi apa yang mungkin digunakan sebagai bukti, baik untuk prosedur kedisiplinan internal atau tindakan hukum.

Fasilitas yang diperlukan untuk analisis forensik dapat digolongkan kedalam fasilitas teknis (misalnya alat audit, fasilitas perolehan bukti), prosedural, personil dan kantor yang aman. Tiap kegiatan analisis forensik harus didokumentasikan sepenuhnya, termasuk foto-foto yang relevan, laporan analisis jejak audit, buku penemuan kembali data. Kecakapan orang atau orang-orang yang melakukan analisis forensik harus didokumentasikan bersama dengan arsip pengujian kecakapan. Informasi lainnya yang dapat menunjukkan obyektifitas dan sifat logis analisis harus didokumentasikan juga. Semua arsip, mengenai insiden keamanan informasi itu sendiri, kegiatan analisis forensik, dll., dan media yang terkait, harus disimpan dalam lingkungan yang aman secara fisik dan dikendalikan dengan memeriksa prosedur yang sedemikian rupa sehingga tidak bisa diakses orang-orang tidak berhak atau diubah atau dibuat tidak tersedia. Alat analisis forensik berdasarkan TI harus sesuai dengan standar sedemikian rupa sehingga ketelitiannya tidak dapat dipermasalahkan secara hukum, serta selalu dijaga *up-to-date* sejalan dengan perubahan teknologi. Lingkungan fisik ISIRT harus menyediakan kondisi-kondisi yang dapat dibuktikan yang memastikan bukti ditangani sedemikian rupa sehingga tidak dapat dipermasalahkan. Personil yang cukup harus tersedia, jika perlu berdasarkan panggilan agar dapat meanggapi setiap waktu.

Dari waktu ke waktu tidak diragukan akan adanya persyaratan untuk meninjau ulang bukti dalam konteks berbagai insiden keamanan informasi, meliputi penipuan, pencurian, dan vandalisme. Jadi, untuk membantu ISIRT diperlukan tersedia sejumlah sarana berbasis TI dan prosedur pendukung untuk membongkar informasi 'yang tersembunyi' dalam sistem informasi, layanan atau jaringan, termasuk informasi yang pada kesempatan pertama nampak seperti telah dihapus, dienkripsi, atau rusak. Sarana ini harus bisa menangani semua aspek yang diketahui yang terkait dengan jenis-jenis insiden keamanan informasi yang dikenali (dan tentu saja didokumentasikan dalam Prosedur ISIRT).

Dalam lingkungan masa kini, analisis forensik sering harus terdiri dari lingkungan-lingkungan yang membentuk jaringan yang kompleks, dimana penyelidikan harus meliputi seluruh lingkungan operasi berbagai jenis *server* - file, cetak, komunikasi, e-mail dll., serta fasilitas akses jarak jauh. Ada banyak alat yang tersedia, alat pencari teks, perangkat lunak penyalin drive dan forensik. Perlu ditekankan disini bahwa fokus utama prosedur analisis forensik adalah untuk memastikan bahwa bukti dijaga tetap utuh dan diperiksa untuk memastikan bahwa bukti akan sah terhadap setiap permasalahan hukum, dan analisis forensik harus

dilakukan tepat pada salinan serupa dari data asli, untuk mencegah pekerjaan analisis karena keraguan atas integritas media yang asli.

Keseluruhan proses analisis forensik harus terdiri dari, bila relevan, kegiatan yang berikut:

- memastikan bahwa sistem target, layanan dan/atau jaringan dilindungi selama analisis forensik dari keadaan yang dianggap tidak tersedia, diubah atau dikompromikan, termasuk pencegahan virus, dan tidak mempengaruhi operasi normal,
- memprioritaskan 'penangkapan' atas 'bukti' yaitu memproses dari bukti yang paling mudah hilang sampai dengan yang paling susah hilang (ini akan tergantung sebagian besar pada sifat insiden keamanan informasi),
- mengidentifikasi semua file yang relevan pada sistem, layanan dan/atau jaringan subyek, termasuk file normal, jelasnya (tetapi bukan) file yang terhapus, kata kunci atau file yang diproteksi, dan file yang dienskripsi,
- pemulihan sebanyak mungkin file terhapus yang ditemukan, dan data yang lain,
- pengungkapan alamat IP, nama *host*, rute jaringan dan informasi situs Web,
- pengekstraksian isi file tersembunyi (*hidden)*, temporer (*temporary*) dan saling dipertukar kan (*swap*) yang digunakan oleh perangkat lunak aplikasi dan sistem operasi,
- pengaksesan isi file yang terenkripsi atau dilindungi (kecuali jika dilarang menurut hukum),
- Menganalisa semua data relevan yang mungkin ditemukan dalam area khusus pada cakram penyimpanan (biasanya tidak dapat diakses),
- Menganalisa akses, modifikasi dan waktu pembuatan file,
- Menganalisa catatan sistem/layanan/jaringan dan aplikasi,
- penentuan aktifitas pemakai dan/atau aplikasi pada sistem/layanan/jaringan,
- Menganalisa informasi sumber dan isi e-mail,
- Melakukan pemeriksaan integritas file untuk mendeteksi file kuda Troya dan file yang awalnya tidak ada pada sistem,
- Menganalisa, jika mungkin, bukti fisik, sebagai contoh sidik jari, kerusakan properti, video pengintai, catatan sistem alarm, catatan akses kartu pass, dan wawancara dengan saksi,
- memastikan bahwa bukti potensial yang telah diekstraksi ditangani dan disimpan sedemikian rupa sehingga tidak bisa dirusak atau dibuat tak dapat dipakai, dan material yang sensitif tersebut tidak bisa dilihat oleh mereka yang tidak berhak. Perlu ditekankan bahwa bukti yang dikumpulkan suatu harus selalu sesuai dengan ketentuan pengadilan atau dengar pendapat dimana bukti mungkin ditunjukkan,
- kesimpulan tentang alasan insiden keamanan informasi, tindakan yang diperlukan dan dalam kerangka waktu apa, dengan bukti yang meliputi daftar file yang relevan yang dimasukkan dalam lampiran laporan utama,
- sebagaimana diperlukan, penyediaan tenaga ahli untuk tindakan kedisiplinan dan hukum.

Metoda yang akan diikuti harus didokumentasikan dalam Prosedur ISIRT.

ISIRT harus mengakomodasi kombinasi ketrampilan yang cukup untuk menyediakan cakupan pengetahuan teknis yang luas (termasuk alat dan teknik yang mungkin akan digunakan oleh penyerang yang sengaja), pengalaman analisis/investigatif (termasuk pemeliharaan bukti yang dapat dipakai), pengetahuan tentang perundang-undangan yang relevan dan implikasi peraturan, dan pengetahuan yang berkelanjutan tentang kecenderungan insiden.

8.5.6 Komunikasi

Dalam banyak kesempatan jika suatu insiden keamanan informasi telah ditetapkan oleh ISIRT adalah benar, maka perlu untuk memberitahu orang-orang secara internal (di luar jalur komunikasi ISIRT/pengelola) dan secara eksternal- termasuk Pers. Ini mungkin harus terjadi pada sejumlah tahapan, sebagai contoh ketika suatu insiden keamanan informasi ditetapkan

benar terjadi, ketika dikonfirmasikan dibawah kendali, ketika ditunjuk untuk kegiatan 'krisis', ketika insiden diselesaikan, ketika tinjauan pasca insiden telah diselesaikan dan kesimpulan dicapai.

Untuk membantu kegiatan ini ketika diperlukan, adalah praktek yang masuk akal untuk menyiapkan informasi tertentu lebih awal sedemikian rupa sehingga dapat dengan cepat disesuaikan kepada keadaan insiden keamanan informasi tertentu dan disampaikan kepada Pers dan/atau Media yang lain. Bila ada informasi yang menyinggung insiden keamanan informasi disampaikan kepada Pers maka itu harus dilakukan sesuai dengan kebijakan penyebaran informasi organisasi. Informasi yang disebarkan harus ditinjau oleh pihak-pihak terkait, yang meliputi pengelola senior, koordinator hubungan masyarakat dan personil keamanan informasi.

8.5.7 Eskalasi

Ada keadaan dimana berbagai hal harus dieskalasi baik kepada pengelola senior, kelompok lain dalam organisasi atau orang atau kelompok di luar organisasi. Ini mungkin untuk suatu keputusan yang akan dibuat tentang tindakan yang direkomendasikan untuk menangani insiden keamanan informasi atau penilaian lebih lanjut untuk menentukan tindakan yang diperlukan. Ini bisa mengikuti proses penilaian yang diuraikan di atas dalam butir 8.4, atau selama proses tersebut jika beberapa isu utama menjadi jelas sejak awalnya. Pedoman harus tersedia dalam dokumentasi skema pengelolaan insiden keamanan informasi bagi mereka yang mungkin pada titik tertentu harus dieskalasi berbagai hal, yaitu. kelompok pendukung operasi dan anggota ISIRT.

8.5.8 Kegiatan pencatatan, dan kendali perubahan

Perlu ditekankan bahwa semua yang terlibat dalam pelaporan dan pengelolaan dari suatu insiden keamanan informasi harus dengan baik mencatat semua kegiatan untuk analisis di kemudian hari. Ini harus termasuk dengan formulir pelaporan insiden keamanan informasi dan dalam basis data kejadian/insiden keamanan informasi, secara terus menerus dimutakhirkan selama daur insiden keamanan informasi dari formulir pelaporan yang pertama hingga penyelesaian pasca peninjauan ulang insiden tersebut. Informasi ini harus disimpan dengan cara yang terbukti aman dan dengan suatu mekanisma back up yang memadai. Lebih lanjut, semua perubahan yang dibuat dalam konteks penjejakan insiden keamanan informasi dan pemutakhiran formulir pelaporan insiden keamanan informasi dan basis data kejadian/insiden keamanan informasi harus di bawah skema kendali perubahan yang diterima secara formal.

9 Peninjauan ulang

9.1 Pendahuluan

Sekali insiden keamanan informasi telah dipecahkan dan penutupan disetujui, kemudian akan ada analisis forensik lebih lanjut, dan peninjauan ulang untuk mengidentifikasi pelajaran dan perbaikan potensial untuk keseluruhan keamanan dan untuk skema pengelolaan insiden keamanan informasi.

9.2 Analisis Forensik Lebih lanjut

Mungkin saja bila suatu insiden telah dipecahkan ada kebutuhan untuk melakukan analisis forensik lebih lanjut untuk mengidentifikasi bukti. Ini harus dilakukan oleh ISIRT menggunakan peralatan dan prosedur yang sama sebagaimana diberikan dalam butir 8.5.5.

9.3 Pengalaman

Sekali insiden keamanan informasi ditutup, adalah penting bahwa pengalaman dari proses penanganan insiden keamanan informasi diidentifikasikan dan dilakukan tindakan dengan cepat. Pengalaman bisa dalam bentuk:

- persyaratan baru atau yang diubah untuk perlindungan keamanan informasi. Ini bisa jadi perlindungan teknis atau nonteknis (termasuk fisik). Tergantung pada pengalaman, ini bisa meliputi kebutuhan pemutakhiran material yang cepat, dan penyerahan, pengarahan singkat kesadaran keamanan (untuk pemakai serta personil lainnya), dan revisi cepat dan penerbitan panduan keamanan dan/atau standar,
- dan/atau perubahan kepada skema pengelolaan insiden keamanan informasi dan prosesnya, formulir pelaporan dan basis data kejadian/insiden keamanan informasi.

Lebih lanjut, dalam kegiatan ini diperlukan untuk melihat di luar insiden keamanan informasi yang tunggal dan memeriksa kecenderungan/pola yang bisa membantu mengidentifikasi kebutuhan perlindungan atau perubahan pendekatan. Ini juga praktek lazim mengikuti suatu insiden keamanan informasi yang berorientasi TI, melakukan pengujian keamanan informasi, terutama sekali penilaian kerentanannya.
Jadi, data dalam basis data kejadian/insiden keamanan informasi harus dianalisis secara berkala dalam rangka:

- mengidentifikasi kecenderungan/pola,
- mengidentifikasi bidang yang perlu diperhatikan,
- menganalisis di mana tindakan pencegahan bisa diambil untuk mengurangi kemungkinan terjadinya insiden di masa depan.

Informasi yang relevan yang diperoleh sepanjang insiden keamanan informasi harus disalurkan ke dalam analisis kecenderungan/pola analisis. Ini dapat memberikan sumbangan yang signifikan kepada identifikasi awal dari insiden keamanan informasi dan memberikan peringatan mengenai insiden keamanan informasi lebih lanjut apa yang mungkin timbul, berdasarkan pada pengalaman sebelumnya dan pengetahuan yang terdokumentasikan.

Penggunaan harus juga dibuat dari insiden keamanan informasi dan informasi kerentanan terkait yang diterima dari pemerintah, CERT komersial dan para pemasok.

Penilaian kerentanan/pengujian keamanan sistem, layanan dan/atau jaringan informasi yang mengikuti insiden keamanan informasi, harus tidak terbatas hanya pada sistem, layanan dan/atau jaringan informasi, yang terkena oleh insiden keamanan informasi. Pengujian harus diperluas untuk meliputi sistem, layanan dan/atau jaringan informasi terkait. Penilaian kerentanan yang lengkap digunakan untuk menyoroti adanya kerentanan yang dieksploitasi selama insiden keamanan informasi tentang sistem, layanan dan/atau jaringan informasi lainnya dan untuk memastikan bahwa tidak ada kerentanan baru.

Perlu ditekankan bahwa penilaian kerentanan itu harus dilakukan secara berkala, dan penilaian kembali kerentanan setelah insiden keamanan informasi terjadi harus merupakan bagian dari proses penilaian yang berlanjut ini (dan bukan sebagai pengganti).

Ringkasan analisis insiden keamanan informasi harus dihasilkan untuk pentabelan pada setiap rapat forum pengelola keamanan informasi organisasi dan/atau forum lain yang didefinisikan dalam kebijakan keamanan informasi organisasi keseluruhan.

9.4 Identifikasi Perbaikan Keamanan

Selama peninjauan ulang setelah insiden keamanan informasi dipecahkan, perlindungan baru yang diubah bisa diidentifikasikan sebagaimana diperlukan. Rekomendasi dan persyaratan perlindungan yang terkait mungkin sedemikian rupa sehingga tidak layak secara finansial dan operasional menerapkannya segera, dalam hal mana mereka harus digambarkan dalam tujuan jangka panjang organisasi. Sebagai contoh, migrasi kepada *firewall* yang lebih kuat dan aman mungkin secara finansial tidak layak dalam jangka pendek, tetapi diperlukan untuk dijadikan faktor dalam sasaran keamanan jangka panjang. (Lihat juga butir 10.3 di bawah.)

9.5 Identifikasi Perbaikan Skema

Penyelesaian pasca-insiden, pengelola ISIRT atau calon harus meninjau ulang semua yang telah terjadi untuk menilai dan dengan begitu ‘mengukur' efektivitas seluruh tanggapan kepada insiden keamanan informasi. Analisis seperti itu bertujuan untuk menentukan bagian yang mana dari skema pengelolaan insiden keamanan informasi yang dikerjakan dengan sukses dan mengidentifikasi bila ada perbaikan yang diperlukan.

Suatu aspek penting tentang analisis pasca tanggapan adalah mengumpankan balik informasi dan pengetahuan ke dalam skema pengelolaan insiden keamanan informasi. Bila kerusakannya cukup parah, maka suatu pertemuan semua pihak terkait harus dijadwalkan segera sesudah resolusi insiden selagi informasi masih segar dalam ingatan. Faktor-faktor yang dipertimbangkan dalam pertemuan tersebut meliputi hal berikut:

- apakah prosedur yang diuraikan dalam skema pengelolaan insiden keamanan informasi bekerja sebagaimana diharapkan?
- adakah prosedur atau metoda yang mungkin dapat membantu pendeteksian insiden?
- apakah prosedur atau peralatan yang diidentifikasikan itu telah membantu dalam proses tanggapan?
- adakah prosedur yang telah membantu pemulihan sistem informasi setelah suatu insiden diidentifikasikan?
- adakah komunikasi insiden yang efektif kepada semua pihak terkait sepanjang proses pendeteksian, pelaporan dan tanggapan?

Hasil pertemuan harus didokumentasikan dan tindakan yang disetujui dilaksanakan dengan sewajarnya (lihat butir 10.4 di bawah).

10 Perbaikan

10.1 Pendahuluan

Tahap “Perbaikan” meliputi pelaksanaan rekomendasi dari tahap "Tinjauan", yaitu untuk perbaikan kepada analisis resiko keamanan dan hasil pengelolaan, kepada keamanan dan kepada skema pengelolaan insiden keamanan informasi. Tiap topik ini dibahas dalam butir di bawah ini.

10.2 Analisis resiko keamanan dan perbaikan manajemen

Tergantung pada kerusakan dan dampak buruk dari insiden keamanan informasi, suatu penilaian dari analisis resiko keamanan informasi dan hasil tinjauan manajemen mungkin perlu mempertimbangkan ancaman dan kerentanan baru. Sebagai kelanjutan kepada penyelesaian analisis resiko keamanan informasi yang dimutakhirkan dan tinjauan manajemen, mungkin perlu untuk memperkenalkan perlindungan yang diubah atau perlindungan baru.

10.3 Membuat perbaikan keamanan

Sebagai kelanjutan dari rekomendasi yang dibuat sepanjang tahap "Tinjauan" (lihat butir 9.4 di atas), dan analisis sejumlah insiden keamanan informasi, implementasi dari perlindungan yang baru dan/atau dimutakhirkan perlu dimulai. Seperti dibahas dalam butir 9.3 di atas, ini bisa perlindungan teknis (mencakup fisik), dan bisa meliputi kebutuhan akan pemutakhiran cepat material, dan penyerahan, pengarahan singkat kesadaran keamanan (untuk pemakai serta personil lain), dan revisi cepat dan penerbitan panduan keamanan dan/atau standar. Lebih lanjut, suatu sistem, layanan dan jaringan informasi organisasi harus tunduk kepada penilaian kerentanan yang berkala untuk membantu identifikasi kerentanan dan menyediakan proses pembakuan sistem/layanan/jaringan berkesinambungan.

Sebagai tambahan, selagi tinjauan prosedur dan dokumentasi terkait keamanan informasi bisa dilakukan segera setelah suatu insiden, mungkin ini akan diperlukan sebagai tanggapan lanjutan. Setelah insiden keamanan informasi, jika kebijakan dan prosedur keamanan informasi yang relevan harus dimutakhirkan dengan mempertimbangkan informasi yang telah dikumpulkan dan permasalahan yang diidentifikasikan sepanjang proses pengelolaan insiden tersebut. Hal itu akan merupakan tujuan jangka panjang ISIRT, bersama dengan pengelola keamanan informasi organisasi, untuk memastikan bahwa kebijakan keamanan informasi ini dan pemutakhiran prosedural disebarkan ke seluruh organisasi.

10.4 Membuat perbaikan skema

Bidang yang diidentifikasikan untuk perbaikan skema pengelolaan insiden keamanan informasi (lihat butir 9.5 di atas) harus ditinjau ulang dan perubahan yang dibenarkan disatukan ke dalam dokumentasi skema yang dimutakhirkan. Perubahan atas proses, prosedur dan formulir pelaporan pengelolaan insiden keamanan informasi, harus tunduk kepada pengujian dan pemeriksaan yang seksama sebelum digunakan.

10.5 Perbaikan lain

Perbaikan mungkin telah diidentifikasikan selama tahap "Tinjauan", sebagai contoh, perubahan dalam kebijakan keamanan, standar dan prosedur informasi, dan perubahan konfigurasi perangkat keras dan lunak TI.

11 Ringkasan

Standar ini memberikan ikhtisar pengelolaan insiden keamanan informasi, keuntungan pengadopsian skema pengelolaan insiden keamanan informasi, dan hal-hal penting yang dihubungkan dengan pengadopsian skema tersebut. Langkah yang jelas menyangkut perencanaan dan pendokumentasian kebijakan dan skema pengelolaan insiden keamanan informasi dirinci bersama dengan proses dan prosedur terkait untuk pengelolaan insiden keamanan informasi, dan melakukan kegiatan resolusi pasca-insiden.

Lampiran A
(Informatif)

Contoh formulir laporan kejadian dan insiden keamanan informasi

Laporan Kejadian dan Insiden Keamanan Informasi

Catatan untuk pengisian

Tujuan formulir ini – formulir laporan kejadian dan insiden keamanan informasi - adalah untuk menyediakan informasi tentang kejadian keamanan informasi, dan kemudian, jika ditetapkan sebagai insiden keamanan informasi, diinformasikan kepada orang-orang yang tepat.

Jika anda mencurigai suatu kejadian keamanan informasi adalah sedang dalam proses atau mungkin telah terjadi - terutama sekali satu yang bisa menyebabkan kerugian atau kerusakan *substansial* pada *property* atau reputasi organisasi, anda harus segera mengisi dan menyerahkan formulir laporan kejadian keamanan informasi (lihat bagian pertama Lampiran ini) sesuai dengan prosedur yang diuraikan dalam skema pengelolaan insiden keamanan informasi dari organisasi.

Informasi yang anda berikan akan digunakan untuk memulai penilaian yang sesuai, yang akan menentukan apakah kejadian digolongkan sebagai insiden keamanan informasi atau tidak, dan jika perlu tindakan perbaikan untuk mencegah atau membatasi kerugian atau kerusakan. Karena sifat proses ini yang kritis waktu, maka tidak penting untuk melengkapi seluruh isian dalam formulir laporan pada waktu ini.

Jika anda adalah anggota kelompok pendukung operasi yang memeriksa formulir yang telah lengkap/terlengkapi sebagian, maka anda akan diminta memberikan pandangan apakah kejadian tersebut perlu digolongkan sebagai insiden keamanan informasi. Jika kejadian digolongkan demikian, anda harus melengkapi formulir insiden keamanan dengan sebanyak mungkin informasi yang dapat anda sampaikan dan meneruskan formulir kejadian dan formulir insiden keamanan informasi kepada ISIRT. Terlepas dari kejadian keamanan informasi digolongkan sebagai suatu insiden atau tidak, basis data kejadian/insiden keamanan informasi harus dimutakhirkan.

Jika anda adalah anggota ISIRT yang memeriksa formulir kejadian dan insiden keamanan informasi yang disampaikan oleh anggota kelompok pendukung operasi, maka formulir insiden harus dimutakhirkan sementara penyelidikan berjalan dan pemutakhiran terkait dilakukan pada basis data kejadian/insiden keamanan informasi.

Silahkan perhatikan panduan yang berikut ketika melengkapi formulir tersebut:

- jika mungkin, formulir harus dilengkapi dan disampaikan secara elektronik[10]. (Jika ada masalah, atau dianggap ada, dengan mekanisme pelaporan elektronik yang baku (misalnya e-mail), termasuk jika dianggap sistem mungkin sedang diserang dan formulir pelaporan bisa dibaca oleh orang-orang yang tidak berhak, maka sarana pelaporan alternatif harus digunakan. Sarana alternatif bisa meliputi orang, dengan telepon atau pesan teks.),

[10] Jika sama sekali memungkinkan formulir ini harus formulir elektronik (mis. dalam halaman web yang aman) dengan pertalian kepada database kejadian/insiden keamanan informasi elektronik. Dalam dunia masa kini, mengoperasikan suatu skema berdasarkan kertas akan menghabiskan waktu dan bukan operasi cara yang paling efisien.

- hanya memberikan informasi yang anda ketahui berdasar fakta - jangan berspekulasi dalam mengisi formulir. Jika pantas memberikan informasi yang tidak dapat anda konfirmasikan, nyatakan dengan jelas bahwa informasi itu tidak dikonfirmasi, dan apa yang membuat anda percaya itu benar,
- anda harus memberikan rincian lengkap tentang kontak anda. Mungkin saja diperlukan untuk menghubungi anda – baik segera maupun kemudian - untuk memperoleh informasi lebih lanjut mengenai laporan anda,

Jika anda kemudian menemukan bahwa informasi yang telah anda berikan tidak akurat, tidak lengkap atau keliru, anda harus memperbaiki dan menyerahkan kembali laporan anda.

Laporan Kejadian Keamanan Informasi

Tanggal Kejadian

Nomor Kejadian:[11]

(Jika Berlaku) Kejadian dan/atau Peristiwa Terkait Nomor Identitas:

RINCIAN PELAPOR

Nama	……..	**Alamat**	……
Organisasi	……..		……..
Telepon	……..	**Email**	……
			……..

URAIAN KEJADIAN KEAMANAN INFORMASI

Uraian Kejadian

- Apa yang terjadi
- Bagaimana terjadi
- Mengapa terjadi
- Komponen yang terpengaruh
- Dampak bisnis kurang baik
- Kelemahan yang diidentifikasikan

RINCIAN KEJADIAN KEAMANAN INFORMASI

Tanggal dan Waktu Kejadian Terjadi

Tanggal dan Waktu Kejadian Diketahui

Tanggal dan Waktu Kejadian Dilaporkan

Apakah Kejadian Berakhir? *(contreng yang sesuai)* **YES** ☐ **NO** ☐

---

[11] *Nomor kejadian harus dialokasikan oleh Manajer organisasi ISIRT*

S

Laporan Insiden Keamanan Informasi

Tanggal Insiden

Nomor Insiden: [12]

(Jika Berlaku) Kejadian dan/atau Insiden terkait Nomor Identitas:

RINCIAN ANGGOTA KELOMPOK PENDUKUNG

Nama	.....	Alamat	.....
Telepon	.....	E-mail	.....

RINCIAN ANGGOTA ISIRT

Nama	.....	Alamat	.....
Telepon	.....	E-mail	.....

PENJELASAN INSIDEN KEAMANAN INFORMASI

Penjelasan Lebih Lanjut Dari Insiden:

- Apa yang terjadi
- Bagaimana terjadinya
- Mengapa terjadi
- Bagian yang terkena
- Dampak yang mempengaruhi bisnis
- Kerentanan yang dapat diidentifikasikan

RINCIAN INSIDEN KEAMANAN INFORMASI

Tanggal dan waktu terjadinya insiden

Tanggal dan waktu menemukan insiden

Tanggal dan waktu melaporkan insiden

Apakah insiden telah berakhir? *(tandai yang sesuai)* **YA** ☐ **TIDAK** ☐

Jika ya, jelaskan berapa lama insiden berakhir dalam hari/jam/menit. Jika tidak, tetapkan berapa lama hal ini telah berlangsung sampai saat ini!

12 (*nomor insiden harus di tetapkan oleh manajer organisasi ISIRT, dan dihubungkan ke nomor kejadian yang sesuai)*

Laporan Insiden Keamanan Informasi

JENIS INSIDEN KEAMANAN INFORMASI

(Pilih salah satu, dan lengkapi pilihan terkait di bawah ini)

Aktual ☐ **Dicoba** ☐ **Dicurigai** ☐

[redacted]

(*Salah satu*) **Disengaja** ☐ (***Sebutkan jenis ancaman yang terlibat***)

Pencurian	**(TH)**	☐	Hacking/Infiltrasi Logika	**(HA)**	☐
Penipuan	**(FR)**	☐	Salah guna Sumber	**(MI)**	☐
Sabotase/Kerusakan Fisik	**(SA)**	☐	Lain-lain	**(OD)**	☐
Kode jahat	**(MC)**	☐	*Sebutkan:*		

(*Salah satu*) **Ketidaksengajaan** ☐ *(sebutkan jenis ancaman yang terlibat)*

Kegagalan Perangkat Keras	**(HF)**	☐	Kejadian Alam Lainnya	**(NE)**	☐
Kegagalan Perangkat Lunak	**(SF)**	☐	*Sebutkan:*		
Kegagalan Komunikasi	**(CF)**	☐	Kehilangan Layanan Penting	**(LE)**	☐
Kebakaran	**(FI)**	☐	Kekurangan Staf	**(SS)**	☐
Banjir	**(FL)**	☐	Lain-lain	**(OA)**	☐

Sebutkan

(*Salah satu*) Kesalahan ☐ *(Sebutkan jenis ancaman yang terlibat)*

Kesalahan Operasi	**(OE)**	☐	Kesalahan Pemakai	**(UE)**	☐
Kesalahan Perawatan Perangkat Keras	**(HE)**	☐	Kesalahan Desain	**(DE)**	☐
Kesalahan Perawatan Perangkat Lunak	**(SE)**	☐	Lain-lain (termasuk cacat asli)	**(OA)**	☐

Sebutkan:

Tidak Diketahui ☐ *(jika belum dapat ditentukan apakah insiden disengaja, tidak disengaja atau kesalahan, beri tanda disini dan bila mungkin sebutkan jenis ancaman yang terkait menggunakan singkatan jenis ancaman di atas)*

Sebutkan:

Laporan Insiden Keamanan Informasi

ASET YANG TERKENA

Assets yang Terkena *(Berikan uraian tentang aset yang terkena atau yang terkait dengan insiden, termasuk nomor seri, lisensi dan versi).*
(bila ada)

Informasi/Data	----------
Perangkat keras	----------
Perangkat lunak	----------
Komunikasi	----------
Dokumentasi	----------

DAMPAK INSIDEN TERHADAP BISNIS

Untuk hal yang berikut ini pilihlah, kenudian terhadap "nilai" catatlah dampak insiden terhadap bisnis, meliputi semua pihak yang terkena oleh Insiden, dengan skala 1 sampai 10 dengan menggunakan pedoman kategori: Kerugian Keuangan dari Operasi Bisnis (FD), Kepentingan Komersial dan Ekonomi (CE), Informasi Pribadi (PI), Kewajiban Hukum dan Regulasi (LE), Operasi Pengelolaan dan Bisnis (MO), dan Kehilangan Reputasi Baik (LG). (Lihat Lampiran B untuk contoh) Catat huruf kode untuk pedoman yang sesuai di bawah "Pedoman", dan jika biaya aktual diketahui masukkan dalam kolom "biaya".

	Nilai	Pedoman	Biaya
Pelanggaran kerahasiaan (*yaitu, pengungkapan yang tidah sah*)	☐		
Pelanggaran Integritas (*yaitu, modifikasi yang tidak sah*)	☐		
Pelanggaran Ketidaktersediaan (*yaitu, ketidaktersediaan*)	☐		
Pelanggaran *Non-Repudiation* (*yaitu, tidak tersanggah*)	☐		
Kerusakan			
Total	☐		

(Bila mungkin, harus ditunjukkan biaya total aktual pemulihan Insiden secara keseluruhan, dibandingkan dengan "nilai" menggunakan skala 1 sampai 10 dan dibandingkan dengan "biaya" aktual)	Nilai	Pedoman	Biaya

Laporan Insiden Keamanan Informasi

RESOLUSI INSIDEN

Tanggal Dimulainya Penyidikan .....

Nama Penyidik Insiden .....

Tanggal Insiden Berakhir .....

Tanggal Dampak Berakhir .....

Tanggal Selesainya Penyidikan Insiden .....

Acuan dan Lokasi dari Laporan Penyidik .....

ORANG/PELAKU YANG TERLIBAT

(salah satu) Orang (OR) ☐ Organisasi/Lembaga Legal (OL) ☐

Kelompok Terorganisir (KT) ☐ Ketidaksengajaan (AC) ☐

Tidak ada pelaku (NP) ☐

Mis. unsur alam, kegagalan peralatan, kesalahan manusia

URAIAN PELAKU

MOTIVASI

(*satu dari*) Kriminal/Keuntungan Keuangan(CG) ☐ Hacking (PH) ☐

Politis/Terorisme (PT) ☐ Tindakan Pembalasan (RE) ☐

Lain-lain (OM) ☐

Sebutkan

TINDAKAN YANG DIAMBIL UNTUK MENYELESAIKAN INSIDEN

(*mis.'tidak ada tindakan', 'tindakan in-house', 'penyidikan internal', penyidikan 'eksternal' oleh..')*

TINDAKAN TERENCANA UNTUK MENYELESAIKAN INSIDEN

(*mis.lihat contoh)*

TINDAKAN YANG BELUM DILAKUKAN

(*mis. penyidikan masih diperlukan oleh personil lain)*

Laporan Insiden Keamanan Informasi

KESIMPULAN

(Beri tanda untuk menunjukkan bahwa Insiden dianggap Major atau Minor , termasuk narasi singkat yang menjustifikasi kesimpulan

Major ☐ Minor ☐

(Sebutkan kesimpulan lain)

INDIVIDU/ENTITAS YANG DIBERITAHU

(Rincian ini diisi oleh orang yang bertanggung jawab terhadap keamanan informasi, untuk menyatakan tindakan yang diperlukan. Hal ini bisa disesuaikan oleh Pengelola Keamanan Informas)i

Pengelola Keamanan Informasi	☐	Pengelola ISIRT	☐
Pengelola lokasi (Sebutkan lokasi mana)	☐	Pengelola Sistem Informasi	☐
Pelapor	☐	Manajer dari Pelapor	☐
Polisi	☐	Lain-lain	☐

(mis. Help Desk, SDM, Manajemen, Audit Internal, Badan Regulator ,CERT Eksternal)

Sebutkan:

INDIVIDU YANG TERLIBAT

PELAPOR	**PEMERIKSA**	**PEMERIKSA**
Tanda tangan	Tanda tangan	Tanda tangan .....
Nama	Nama	Nama .....
Jabatan	Jabatan	Jabatan .....
Tanggal	Tanggal	Tanggal

PEMERIKSA	**PEMERIKSA**	**PEMERIKSA**
Tanda tangan	Tanda tangan	Tanda tangan .....
Nama	Nama	Nama .....
Jabatan	Jabatan	Jabatan .....
Tanggal	Tanggal	Tanggal

Lampiran B
(informatif)

Contoh garis besar panduan untuk penilaian insiden keamanan informasi

B. 1 Pendahuluan

Lampiran ini menyajikan contoh garis besar panduan untuk penilaian dan penggolongan konsekuensi yang buruk dari insiden keamanan informasi, dengan tiap panduan menggunakan skala: 1 (rendah) sampai 10 (tinggi). (Dalam praktek dapat digunakan skala lain, katakan 1 sampai 5, dan tiap organisasi harus mengadopsi skala yang paling cocok untuk lingkungannya).

Sebelum membaca panduan di bawah ini, penjelasan berikut harus dicatat:

- pada beberapa contoh garis besar disusun seperti di bawah ini, beberapa entri diberi catatan "Tidak ada entri". Hal ini karena panduan diformulasikan sedemikian rupa sehingga konsekuensi yang merugikan pada tiap tahap naik, dinyatakan pada skala 1 sampai 10, secara umum serupa pada semua enam kategori yang ditunjukkan. Meskipun demikian, pada beberapa tahap (pada skala 1 sampai 10) untuk beberapa kategori, dianggap tidak ada perbedaan yang cukup atas konsekuensi entri yang lebih rendah untuk membuat suatu entri – dan ini diberi catatan "Tidak ada entri". Demikian juga, pada ujung yang lebih tinggi beberapa kategori dianggap tidak ada konsekuensi yang lebih besar daripada entri tertinggi yang ditunjukkan – jadi entri tertinggi diberi catatan "Tidak ada entri". (Jadi, logisnya tidak benar menghilangkan jalur "Tidak ada entri" dan mengecilkan skala.),
- untuk panduan di bawah yang menggunakan angka finansial, julat yang ditunjukkan akan nampak aneh. Sebelum penggunaan, panduan ini perlu dilengkapi dengan julat angka finansial yang menggunakan mata uang yang sesuai untuk organisasi.

Jadi, penggunaan yang berikut ini sebagai contoh panduan ketika mempertimbangkan konsekuensi yang buruk dari insiden keamanan informasi pada bisnis suatu organisasi, dari:

- pengungkapan informasi yang tidak sah,
- perubahan informasi yang tidak sah,
- penyanggahan dari informasi,
- ketidak-tersediaan informasi atau layanan,
- perusakan informasi dan/atau layanan,

Langkah pertama adalah mempertimbangkan yang mana dari kategori berikut yang relevan. Untuk yang dianggap relevan, panduan kategori harus digunakan untuk membuat dampak buruk yang aktual atas operasi bisnis (atau "nilai") untuk entri ke dalam formulir pelaporan insiden keamanan informasi.

B.2 Kerugian/disrupsi finansial pada operasi bisnis

Konsekuensi dari modifikasi dan penyingkapan yang tidak sah, penyanggahan, serta ketidak-tersediaan dan pengrusakan informasi seperti itu, bisa menjadi kerugian finansial, misalnya dari pengurangan harga saham, penipuan atau pelanggaran perjanjian oleh karena tidak ada atau terlambatnya tindakan. Dengan kata lain, konsekuensi dari ketidak-tersediaan atau pengrusakan informasi bisa menjadi gangguan bagi operasi bisnis. Untuk mengoreksi dan/atau memulihkan dari insiden seperti itu akan memerlukan waktu dan

usaha. Ini akan menjadi hal penting dan harus dipertimbangkan. Dalam rangka penggunaan pembagi umum, waktu pemulihan harus dihitung untuk unit waktu personil dan dikonversikan menjadi biaya finansial. Biaya ini harus dihitung dengan mengacu kepada biaya normal untuk orang bulan (person month) pada tingkat yang sesuai di dalam organisasi. Panduan yang berikut harus digunakan.

1. Mengakibatkan kerugian/biaya finansial x_1 atau kurang
2. Mengakibatkan kerugian/biaya finansial antara $x_1 + 1$ dan x_2
3. Mengakibatkan kerugian/biaya finansial antara $x_2 + 1$ dan x_3
4. Mengakibatkan kerugian/biaya finansial antara $x_3 + 1$ dan x_4
5. Mengakibatkan kerugian/biaya finansial antara $x_4 + 1$ dan x_5
6. Mengakibatkan kerugian/biaya finansial antara $x_5 + 1$ dan x_6
7. Mengakibatkan kerugian/biaya finansial antara $x_6 + 1$ dan x_7
8. Mengakibatkan kerugian/biaya finansial antara $x_7 + 1$ dan x_8
9. Mengakibatkan kerugian/biaya finansial lebih dari x_8
10. Organisasi akan keluar dari bisnis

B.3 Kepentingan komersial dan ekonomi

Informasi komersial dan ekonomi perlu dilindungi, dan dinilai dengan mempertimbangkan nilainya dengan pesaing atau efek kompominya bisa pada kepentingan komersial. Panduan yang berikut harus digunakan.

1. Merupakan kepentingan bagi pesaing tetapi tidak mempunyai nilai komersial.
2 Merupakan kepentingan bagi pesaing kepada nilai y_1 atau kurang (perputaran)
3 Menjadi bernilai bagi pesaing untuk nilai antara $y_1 + 1$ dan y_2 (perputaran), atau menyebabkan kerugian finansial, atau hilangnya pendapatan potensial, atau memudahkan keuntungan atau manfaat yang tidak pantas untuk individu atau organisasi, atau mendasari pelanggaran usaha yang sesuai untuk memelihara kepercayaan informasi yang diberikan oleh pihak ketiga
4 Menjadi bernilai bagi pesaing untuk nilai antara $y_2 + 1$ dan y_3 (perputaran)
5 Menjadi bernilai bagi pesaing untuk nilai antara $y_3 + 1$ dan y_4 (perputaran)
6 Menjadi bernilai bagi pesaing untuk nilai lebih daripada $y_4 + 1$
7 Tidak ada entri[13]
8 Tidak ada entri
9 Bisa secara substansial menurunkan kepentingan komersial, atau menurunkan viabilitas organisasi
10 Tidak ada entri

B.4 Informasi pribadi

Jika informasi individu ditahan dan diproses, secara moral dan secara etis adalah benar, dalam beberapa keadaan secara hukum diperlukan, informasi dilindungi dari penyingkapan yang tidak sah yang bisa memalukan dan paling buruk menjadi tindakan hukum, sebagai contoh di bawah undang-undang perlindungan data. Dengan kata lain diperlukan informasi yang selalu benar tentang orang, sebab modifikasi yang tidak sah yang dapat menghasilkan informasi yang tidak benar bisa mempengaruhi seperti penyingkapan yang tidak sah. Merupakan hal yang penting juga bahwa informasi tentang orang selalu tersedia dan tidak dirusak, karena hal ini dapat menyebabkan keputusan yang salah atau tidak adanya tindakan pada waktu yang dibutuhkan, dengan pengaruh yang sama seperti untuk modifikasi atau penyingkapan yang tidak sah. Panduan berikut harus digunakan.

[13] Istilah 'tidak ada entri' berarti tidak ada entri yang sesuai untuktingkat dapak ini

1 Terjadi ketegangan minor atas individu (kemarahan, frustrasi, kekecewaan) tetapi tidak ada pelanggaran hukum atau persyaratan regulasi
2 Terjadi ketegangan atas individu (kemarahan, frustrasi, kekecewaan) tetapi tidak ada pelanggaran hukum atau persyaratan regulasi
3 Pelanggaran persyaratan hukum, peraturan atau etika atau pengatur atau niat yang dipublikasikan tentang perlindungan informasi, yang menyebabkan kesulitan minor pada individu
4 Pelanggaran persyaratan hukum, peraturan atau etika atau pengatur atau niat yang dipublikasikan tentang perlindungan informasi, yang menyebabkan kesulitan yang signifikan pada individu atau kesulitan kecil pada kelompok individu
5 Pelanggaran persyaratan hukum, peraturan atau etika atau pengatur atau niat yang dipublikasikan tentang perlindungan informasi, yang menyebabkan kesulitan serius pada individu
6 Pelanggaran persyaratan hukum, peraturan atau etika atau pengatur atau niat yang dipublikasikan tentang perlindungan informasi, yang menyebabkan kesulitan serius pada kelompok individu
7 Tidak ada entri
8 Tidak ada entri
9 Tidak ada entri
10 Tidak ada entri

B.5 Kewajiban hukum dan regulasi

Data yang dipegang dan diproses oleh suatu organisasi mungkin harus tunduk kepada, atau dipegang dan diproses dalam rangka mengizinkan organisasi mematuhi, kewajiban hukum dan regulasi. Kegagalan mematuhi kewajiban seperti itu, disengaja atau tidak disengaja, bisa menyebabkan diambilnya tindakan hukum atau administrasi terhadap individu dalam organisasi terkait. Tindakan ini mengakibatkan denda dan/atau hukuman penjara. Panduan yang berikut harus digunakan.

1 Tidak ada entri
2 Tidak ada entri
3 Pemberitahuan Penerapan, perkara perdata atau pelanggaran kriminal yang mengakibatkan kerusakan/denda finansial z_1, atau kurang
4 Pemberitahuan Penerapan, perkara perdata atau pelanggaran kriminal yang mengakibatkan kerusakan/denda finansial antara $z_1 + 1$ dan z_2
5 Pemberitahuan Penerapan, perkara perdata atau pelanggaran kriminal yang mengakibatkan kerusakan/denda finansial antara $z_2 + 1$ dan z_3 atau hukuman penjara sampai dengan dua tahun
6 Pemberitahuan Penerapan, perkara perdata atau pelanggaran kriminal yang mengakibatkan kerusakan/denda finansial antara $z_3 + 1$ dan z_4 atau hukuman penjara lebih dua tahun sampai dengan sepuluh tahun
7 Pemberitahuan Penerapan, perkara perdata atau pelanggaran kriminal yang mengakibatkan kerusakan/denda finansial tak terbatas antara $z_3 + 1$ dan z_4 atau hukuman penjara lebih sepuluh tahun
8 Tidak ada entri
9 Tidak ada entri
10 Tidak ada entri

B.6 Operasi dari manajemen dan bisnis

Informasi bisa sedemikian rupa sehingga kompromi akan merugikan performa efektif suatu organisasi. Sebagai contoh, informasi yang berkaitan dengan perubahan kebijakan bisa mendorong reaksi publik jika disingkapkan, yang akhirya tidak dapat melaksanakan

kebijakan tersebut. Modifikasi, penolakan atau ketidak-tersediaan informasi yang terkait dengan aspek finansial, atau perangkat lunak komputer, dapat juga menimbulkan ramifikasi serius operasi suatu organisasi. Lebih lanjut, penolakan komitmen dapat menimbulkan konsekuensi bisnis yang kurang baik. Panduan yang berikut harus digunakan.

1 Operasi tidak efisien dari satu bagian organisasi
2 Tidak ada entri
3 Merusak pengelolaan dari organisasi dan operasinya
4 Tidak ada entri
5 Menghalangi perkembangan atau operasi yang efektif dari kebijakan organisasi
6 Merugikan organisasi dalam perundingan komersil atau kebijakan dengan pihak lain
7 Menghalangi dengan serius pengembangan atau operasi kebijakan utama organisasi, atau menutup atau jika tidak, mengganggu operasi yang penting
8 Tidak ada entri
9 Tidak ada entri
10 Tidak ada entri

B.7 Kehilangan dari reputasi baik (*goodwill*)

Penyingkapan yang tidak sah, penyanggahan atau modifikasi, atau tentu saja ketidak-tersediaan, dari informasi, bisa mengakibatkan hilangnya reputasi baik organisasi, dengan resultan kerusakan pada reputasi, kehilangan kredibilitas dan konsekuensi yang merugikan lainnya. Panduan yang berikut harus digunakan.

1 Tidak ada entri
2 Menyebabkan malu internal organisasi
3 Secara kurang baik mempengaruhi hubungan dengan pemegang saham, konsumen, pemasok, badan regulasi, pemerintah, organisasi lain atau publik, yang mengakibatkan publisitas lokal/regional yang kurang baik
4. Tidak ada entri
5 Secara kurang baik mempengaruhi hubungan dengan pemegang saham, konsumen, pemasok, badan regulasi, pemerintah, organisasi lain atau publik, yang mengakibatkan beberapa publisitas nasional yang kurang baik
6 Tidak ada entri
7 Secara material mempengaruhi hubungan dengan pemegang saham, konsumen, pemasok, badan regulasi, pemerintah, organisasi lain atau publik, yang mengakibatkan publisitas luas yang kurang baik
8 Tidak ada entri
9 Tidak ada entri
10 Tidak ada entri

Lampiran C
(informatif)

Penyimpangan teknis

Tabel C.1 – Penyimpangan teknis

Butir	ISO/IEC TR 18044:2004	SNI 7512:2008
5.2.3	**Aspek hukum dan regulasi**	**Aspek hukum dan regulasi**
	Tata kearsipan yang terpelihara. Beberapa hukum nasional menyatakan perusahaan diwajbkan memelihara arsip tentang kegiatan mereka untuk peninjauan ulang pada proses audit organisasi tahunan. Persyaratan serupa ada pada organisasi pemerintah. Di beberapa negara organisasi diminta untuk melaporkan atau membuat arsip untuk penerapan hukum (misalnya kasus yang melibatkan kejahatan yang serius atau penetrasi kepada sistem pemerintah yang sensitif).	**Tata kearsipan yang terpelihara.** Perusahaan diwajbkan memelihara arsip tentang kegiatan mereka untuk peninjauan ulang pada proses audit organisasi tahunan. Persyaratan serupa ada pada organisasi pemerintah. Organisasi diminta untuk melaporkan atau membuat arsip untuk penerapan hukum (misalnya kasus yang melibatkan kejahatan yang serius atau penetrasi kepada sistem pemerintah yang sensitif).
	Aspek hukum yang terkait dengan teknik pemantauan harus dijelaskan. Implikasi penggunaan teknik pemantauan perlu diperhatikan dalam konteks perundang-undangan yang relevan. Legalitas dari teknik yang berbeda akan bervariasi dari suatu negara ke negara lain. Sebagai contoh, di beberapa negara diperlukan untuk membuat orang sadar bahwa pemantauan kegiatan sedang berlangsung, termasuk melalui teknik pengawasan. Faktor yang perlu dipertimbangkan meliputi siapa/apa yang dipantau, bagaimana ia dipantau, dan kapan pemantauan terjadi. Perlu juga dicatat bahwa pemantauan/pengintaian dalam konteks IDS (*Intrusion Detection System*) dibahas secara rinci dalam TR 18043.	**Aspek hukum yang terkait dengan teknik pemantauan harus dijelaskan**. Implikasi penggunaan teknik pemantauan perlu diperhatikan dalam konteks perundang-undangan yang relevan. Faktor yang perlu dipertimbangkan meliputi siapa/apa yang dipantau, bagaimana ia dipantau, dan kapan pemantauan terjadi. Perlu juga dicatat bahwa pemantauan/pengintaian dalam konteks IDS (*Intrusion Detection System*) dibahas secara rinci dalam TR 18043.

Bibliografi

ISO/IEC TR 13335-3, *Information technology - Guiedlines for the management of IT SecurityPart 3:Techniques for the management of IT Security*

ISO/IEC TR 15947:2002, *Information technology – Security techniques – IT instrusion detection framework*

ISO/IEC 18028 (all parts), *IT security techniques*

ISO/IEC 18043, *IT security techniques – Guidelines for the Selection, Development and Operations of Instrution Detection System(IDS (document type subject to NP approval on SC27 N4029 by 2004-09-24)*

ISO/IEC Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standars*

Internet Engineering Task Force (IETF) Site Security Handbook, http://www.ietf.org/rfc/rfc2196.txt?number=2196

Expectations for Computer Security incident Response – Best Practice, June 98, ftp://ftp.isi.edu/in-notes/rfc2350.txt

NIST Special Publication 800-3 nov'91, Establishing a Computer Incident Response Capability(CSIRC), http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf

BADAN STANDARDISASI NASIONAL - BSN
Gedung Manggala Wanabakti Blok IV Lt. 3-4
Jl. Jend. Gatot Subroto, Senayan Jakarta 10270
Telp: 021- 574 7043; Faks: 021- 5747045; e-mail : bsn@bsn.go.id